

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2004 年 8 月 5 日 (05.08.2004)

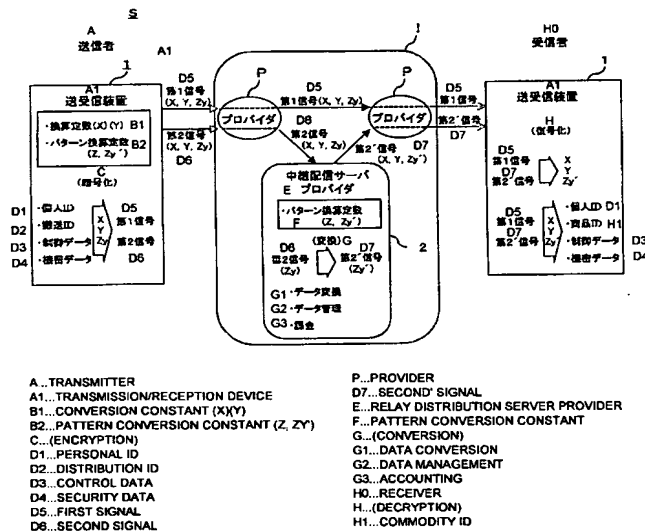
PCT

(10) 国際公開番号
WO 2004/066508 A2

- (51) 国際特許分類⁷: H04B (74) 代理人: 秋山 敦, 外(AKIYAMA, Atsushi et al.); 〒105-0001 東京都港区虎ノ門3丁目5番1号虎ノ門37森ビル Tokyo (JP).
- (21) 国際出願番号: PCT/JP2004/000369
- (22) 国際出願日: 2004 年 1 月 19 日 (19.01.2004) (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2003-10183 2003 年 1 月 17 日 (17.01.2003) JP
- (71) 出願人 および (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, (続葉有)
- (72) 発明者: 加藤 誠 (KATO, Makoto) [JP/JP]; 〒125-0041 東京都葛飾区東金町1-3 6-1-1 3 1 8 Tokyo (JP).

(54) Title: DATA TRANSMISSION SYSTEM, DATA TRANSMISSION METHOD, AND DEVICE

(54) 発明の名称: データ送信システム及びデータ送信方法並びに装置



(57) Abstract: A first signal S_1 containing encrypted data based on a conversion constant $Y.Zy'$ and a conversion constant X is transmitted from a transmission side device (1) to a reception side device (1). A second signal S_2 containing encryption data based on the conversion constant $X.Zy'$, a conversion constant Y , and a pattern conversion constant Zy of the conversion constant Zy' is transmitted from the transmission side device (1) to a relay device (2). A second' signal S_2' in which the pattern conversion constant Zy of the second signal S_2 is converted into a conversion constant Zy' is transmitted from the relay device (2) to the reception side device (1). The reception side device (1) reads the encrypted data and the conversion constants X, Y, Zy' by the first signal S_1 and the second' signal S_2' and performs decryption and authentication of the encrypted data.

(57) 要約: 送信側装置1から受信側装置1へ換算定数 $Y.Zy'$ による暗号化データと、換算定数 X と、を含む第1信号 S_1 が送信され、送信側装置1から中継装置2へ換算定数 $X.Zy'$ による暗号化データと、換算定数 Y と、換算定数 Zy' のパターン換算定数 Zy と、を含む第2信号 S_2 が送信され、第2信号 S_2 のパターン換算定数 Zy が換算定数 Zy' へ変換された第2'信号 S_2' が中継装

(続葉有)



KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

- 国際調査報告書なし；報告書を受け取り次第公開される。

明 細 書

データ送信システム及びデータ送信方法並びに装置

技術分野

- 5 本発明は、データ送信する際に送信データが漏洩した場合においても、その復号化が困難であると共に、第三者の成りすまし送信による不都合を回避できるデータ送信システム及びデータ送信方法並びに装置に関する。

背景技術

- 10 従来から、送信者側で送信すべきデータの暗号化を行い、該暗号化データと該暗号化データを復号化するための暗号鍵とを別々の回線（例えば、衛星通信回線と地上回線）によって受信者側へ送信する技術がある。（日本特許第3052322号公報参照）。

- 15 受信者側では、暗号化されたデータと暗号鍵とを別々に受信し、これらにより元のデータを復号化することができる。このように別々の回線で暗号化データと暗号鍵が送信されることにより、データ送信の秘匿性を高めることができる。

しかし、受信者は、暗号鍵と暗号化されたデータの送信者を認証することなくデータを受信するため、本来送信するはずの送信者に成り代わって第三者によって送信されても送信データを認証することができなかった。

- 20 インターネット等の通信回線上においては、個人認証を行う認証サービス会社の個人認証サービスもある。しかし、そのような認証サービス会社による個人認証サービスは高価であり、個人が利用するには不向きであった。

- 本発明は、上記課題を解決するためになされたものであり、本来の送信者になりかわって第三者がデータを送信しても、受信者側で送信データの認証を行
25 うことができ、上記成りすまし送信による不都合を防ぐことができるデータ送信システム及びデータ送信方法並びに装置を提供することにある。

発明の開示

本発明におけるデータ送信システムは、送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数
5 によって暗号化された送信データを送信するデータ送信システムであって、前記送信側装置は、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択する換算定数選択手段と、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記
10 第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成手段と、前記第3の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信
15 号を前記受信側装置へ送信し前記第2信号を中継装置へ送信する送信手段と、を備え、前記中継装置は、前記パターン換算定数に対応する第3の換算定数を記憶する記憶手段と、前記第2信号を受信して該第2信号に含まれるパターン換算定数に対応する前記第3の換算定数に変換して第2'信号を生成する信号生成手段と、前記第2'信号を前記受信側装置へ送信する送信手
20 段と、を備え、前記受信側装置は、前記送信側装置からの前記第1信号及び前記中継装置からの第2'信号を受信して前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数及び前記第3の換算定数を読取る読取手段と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって
25 第1の復号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記

第2'信号を受け入れる認証をする認証手段と、を備えることを特徴とする。

このように本発明によれば、第1信号に含まれる暗号化データを暗号化した第2の換算定数は第2信号に含めて送信され、第2信号に含まれる暗号化データを暗号化した第1の換算定数は第1信号に含めて送信される。

- 5 さらに、第3の換算定数そのものは送信されず、第3の換算定数に対応するパターン換算定数が第2信号に含めて中継装置へ送信される。そして、このパターン換算定数が、中継装置で第3の換算定数へ変換されることにより、第2信号が第2'信号に変換され、受信側へ転送される。

- 10 このように送信することにより、第3者は第1信号及び第2信号の双方を取得したとしてもパターン換算定数が不明であるので、送信データの復号化を行うことはできない。また、第3者が第1信号又は第2'信号の一方を取得したとしても、それぞれの信号には換算定数のすべての換算定数が含まれていないので、復号化を行うことはできない。

- 15 さらに、第3者が第1信号及び第2'信号の双方を取得したとしても、復号化方法を取得しない限り、有意な復号化データを得ることはできない。

以上のように、本発明によれば第3者が暗号化データを不正に取得したとしても、暗号化データの復号化を有意に行うことができず、送信データの秘匿性を高めることができる。

- 20 また、受信側装置では、送信側装置で選択されたパターン換算定数を知らなくても暗号化データを復号化することができる。したがって、送信側装置では複数のパターン換算定数及び換算定数の組合せを設定することにより、複数の受信側装置へ暗号化データを送信する場合にも秘匿性を高めることができる。

- 25 そして、第3者には換算定数による暗号化方法及びパターン換算定数が不明であるため、送信者に成り代わって送信したとしても、受信側装置では有意なデータとして復号化することができないか、復号化データが一致しないので、

成りすまし送信による不都合を回避することができる。

また、本発明のデータ送信システムは、送信側装置から受信側装置へ第1の換算定数、第2の換算定数、第3の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信システム

5 であって、前記送信側装置は、前記第1の換算定数、前記第2の換算定数、前記第3の換算定数及び前記第4の換算定数を選択する換算定数選択手段と、前記第2の換算定数及び前記第4の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第3の

10 換算定数及び第4の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は前記第4の換算定数に対応するパターン換算定数を含む第1信号を生成する第1信号生成手段と、前記第2の代替値、前記第2の換算定数、及び前記第1信号に含まれない前記第3の換算定数又は前記第4の換算定数の

15 パターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号を第1の中継装置へ送信し前記第2信号を第2の中継装置へ送信する送信手段と、を備え、前記第1の中継装置は、前記パターン換算定数に対応する第3の換算定数又は第4の換算定数を記憶する記憶手段と、前記第1信号を受信して該信号に含まれるパターン換算定数に対応する前記第3の換算

20 定数又は第4の換算定数に変換して第1'信号を生成する信号生成手段と、前記第1'信号を前記受信側装置へ送信する送信手段と、を備え、前記第2の中継装置は、前記パターン換算定数に対応する第3の換算定数又は第4の換算定数を記憶する記憶手段と、前記第2信号を受信して該信号に含まれるパターン換算定数に対応する前記第3の換算定数又は第4の換算定数に

25 変換して第2'信号を生成する信号生成手段と、前記第2'信号を前記受信側装置へ送信する送信手段と、を備え、前記受信側装置は、前記第1'信号及

び前記第2'信号を受信して前記第1'信号から前記第1の代替値、前記第1の換算定数及び前記第3の換算定数又は第4の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数及び前記第3の換算定数又は第4の換算定数を読取る読取手段と、前記第1の代替値及び前記第2の代替値
5 をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の複合化データと前記第2の復号化データから前記第1'信号及び前記第2'信号を受け入れる認証をする認証手段と、を備えることを特徴とする。

このように本発明によれば、第1信号も中継装置を介して受信側装置へ転
10 送される。これにより、さらにデータ送信の秘匿性が高まり、又、より効果的に成りすまし送信による不都合を排除することができる。

また、本発明のデータ送信システムは、送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、前
15 記送信側装置は、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択する換算定数選択手段と、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号
20 化手段と、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成手段と、前記第3の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号及び前記第2信号を前記受信側装置へ送信する送信手段と、を備え、前記
25 受信側装置は、前記第1信号及び前記第2信号を受信して前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2信号から前記第2の代

替値、前記第2の換算定数及び前記パターン換算定数を読取る読取手段と、
前記パターン換算定数に対応する第3の換算定数を記憶する記憶手段と、前
記読取られたパターン換算定数から前記第3の換算定数を読取る手段と、前
記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算
5 定数によって第1の復号化データ及び第2の復号化データへ復号化する復号
化手段と、前記第1の複合化データと前記第2の復号化データから前記第1
信号及び前記第2信号を受け入れる認証をする認証手段と、を備えることを
特徴とする。

このように本発明によれば、中継装置を設けることなく、中継装置が行ってい
10 たパターン換算定数を換算定数に変換する処理を受信側装置で行うように構
成されている。このようにすることにより、データの秘匿性を低下させることなく、
また、成りすまし送信による不都合を排除することができると共に、システムの
構成を簡単化することができる。

また、前記暗号化手段は、前記第2の換算定数及び前記第3の換算定数を
15 用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数
及び前記第3の換算定数を用いて前記第2の代替値へ暗号化するように構
成することができる。

また、前記暗号化手段は、前記第2の換算定数を用いて前記送信データを
前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定
20 数を用いて前記第2の代替値へ暗号化するように構成することができる。

また、前記暗号化手段は、前記第2の換算定数及び前記第3の換算定数
を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数
を用いて前記第2の代替値へ暗号化すれば、成りすまし送信による2つの信
号が受信側装置へ送信されてきた場合であっても、それぞれの信号を復号し
25 て得られた復号化データは不一致となるので、成りすまし送信を排除する効果
が高まるので好適である。

また、前記受信側装置は、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出手段を備えれば、本システムのデータ秘匿性及び成りすまし送信排除効果より、本人又は受信信号を認証して外部駆動装置を操作することができるので好適である。

また、前記認証手段は、前記第1の複合化データと前記第2の復号化データが一致したときに前記認証を行うように構成することができる。また、前記送信側装置、前記中継装置及び前記受信側装置は、インターネットを含む通信回線網に接続する構成とすることができる。また、前記送信側装置と受信側装置は、赤外線方式、無線電波方式、光通信方式、有線通信方式のいずれかによって前記信号の送受信を行うことが可能である。

また、本発明のデータ送信方法は、送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、前記送信側装置が、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択するステップと、前記送信側装置が、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化ステップと、前記送信側装置が、前記第1の代替値、及び前記第1の換算定数を含む第1信号を生成する第1信号生成ステップと、前記送信側装置が、前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数に対応するパターン換算定数を含む第2信号を生成する第2信号生成ステップと、前記送信側装置が、前記第1信号を前記受信側装置へ送信し前記第2信号を中継装置へ送信する第1送信ステップと、前記中継装置が、前記第2信号を受信して該第2信号に含まれるパターン換算定数を対応する前記第3の換

算定数に変換して第2'信号を生成する変換ステップと、前記中継装置が、前記第2'信号を前記受信側装置へ送信する第2送信ステップと、前記受信側装置が、前記送信側装置からの前記第1信号及び前記中継装置からの第2'信号を受信して前記第1信号から前記第1の代替値、及び前記第1の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数を読取る読取ステップと、前記受信側装置が、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化ステップと、前記受信側装置が、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2'信号を受け入れる認証をする認証ステップと、を備えるものとすることができる。

また、本発明のデータ送信方法は、送信側装置から受信側装置へ第1の換算定数、第2の換算定数、第3の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信方法であって、前記送信側装置が、前記第1の換算定数、前記第2の換算定数、前記第3の換算定数及び前記第4の換算定数を選択するステップと、前記送信側装置が、前記第2の換算定数、及び前記第4の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化ステップと、前記送信側装置が、前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は前記第4の換算定数に対応するパターン換算定数を含む第1信号を生成する第1信号生成ステップと、前記送信側装置が、前記第2の代替値、前記第2の換算定数、及び前記第1信号に含まれない前記第3の換算定数又は前記第4の換算定数のパターン換算定数を含む第2信号を生成する第2信号生成ステップと、前記送信側装置が、前記第1信号を第1の中継装置へ送信し前記第2信号を第2の中継装置へ送信する第1送信ステップと、前記

- 第1の中継装置及び前記第2の中継装置が、前記第1信号又は前記第2信号を受信して該信号に含まれるパターン換算定数を対応する前記第3の換算定数又は第4の換算定数に変換して第1'信号又は第2'信号を生成する変換ステップと、前記第1の中継装置及び前記第2の中継装置が、前記第1'信号又は前記第2'信号を前記受信側装置へ送信する第2送信ステップと、前記受信側装置が、前記第1'信号及び前記第2'信号を受信して前記第1'信号から前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は第4の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数又は第4の換算定数を読取る読取ステップと、
- 10 前記受信側装置が、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化ステップと、前記受信側装置が、前記第1の複合化データと前記第2の復号化データから前記第1'信号及び前記第2'信号を受け入れる認証をする認証ステップと、を備えるものとしてすることができる。
- 15 また、本発明のデータ送信方法は、送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、前記送信側装置が、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択するステップと、前記送信側装置が、前記第2の換算定数、又は
- 20 前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化ステップと、前記送信側装置が、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成ステップと、前記送信側装置が、
- 25 前記第2の代替値、前記第2の換算定数及び前記第3の換算定数に対応するパターン換算定数を含む第2信号を生成する第2信号生成ステップと、前記

送信側装置が、前記第1信号及び前記第2信号を前記受信側装置へ送信する送信ステップと、前記受信側装置が、前記第1信号及び前記第2信号を受信して前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2信号から前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を読取る読取ステップと、前記受信側装置が、前記読取られたパターン換算定数に対応する前記第3の換算定数を取得する換算定数取得ステップと、前記受信側装置が、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化ステップと、前記受信側装置が、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証ステップと、を備えるものとしてすることができる。

また、前記暗号化ステップでは、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化するようにできる。

また、前記暗号化ステップでは、前記第2の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化するようにできる。

また、前記暗号化ステップでは、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数を用いて前記第2の代替値へ暗号化するようにできる。

また、前記認証ステップの後、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出ステップを備えれば好適である。

また、前記認証ステップでは、前記第1の複合化データと前記第2の復号化データが一致したときに前記認証を行うようにできる。

また、本発明は、第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信する装置であって、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択する
5 換算定数選択処理と、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化処理と、前記第1の代替値、及び前記第1の換算定数を含む第1信号を生成する第1信号生成処理と、
10 前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数に対応するパターン換算定数を含む第2信号を生成する第2信号生成処理と、前記第1信号と前記第2信号をそれぞれ送信する処理と、を行う制御部と、前記第1信号と前記第2信号を外部へ送信する送信部と、を備える装置により実現できる。

15 また、前記制御部は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化する構成とすることができる。

20 また、前記制御部は、前記第2の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化する構成とすることができる。

また、前記制御部は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数を用いて前記第2の代替値へ暗号化する構成とすることができる。

25 また、本発明は、第1の換算定数、第2の換算定数、第3の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを送信す

る装置であって、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記第1の換算定数、前記第2の換算定数、前記第3の換算定数及び前記第4の換算定数を選択する換算定数選択処理と、前記第2の換算定数及び前記第4の換算定数を用いて前記送信データを第1の代替値に暗号化し

5 前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化処理と、前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は前記第4の換算定数に対応するパターン換算定数を含む第1信号を生成する第1信号生成処理と、前記第2の代替値、前記第2の換算定数、及び前記第1信号に含まれない前記第3の換算定数

10 又は前記第4の換算定数のパターン換算定数を含む第2信号を生成する第2信号生成処理と、を行う制御部と、前記第1信号と前記第2信号を外部へ送信する送信部と、を備える装置により実現できる。

また、本発明は、送信データの暗号化に用いられる換算定数に対応するパターン換算定数を含む信号を転送する装置であって、前記換算定数に対応す

15 るパターン換算定数を記憶する記憶部と、前記信号を送受信する送受信部と、受信した前記信号に含まれるパターン換算定数に対応する前記換算定数に変換して前記信号を変換する信号生成処理と、前記変換された信号を転送する処理と、を行う制御部と、を備える装置により実現できる。

また、本発明は、第1の換算定数、第2の換算定数及び第3の換算定数の

20 少なくとも一の換算定数によって暗号化された送信データを含む第1信号と第2'信号を受信して送信データを復号化する装置であって、前記第1信号には、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第1の代替値と、第1の換算定数と、が含まれ、前記第2'信号には、前記第1の換算定数、又は前記第1の換算

25 定数及び前記第3の換算定数を用いて前記送信データが暗号化された第2の代替値と、前記第2の換算定数と、前記第3の換算定数と、が含まれ、前記

第1信号及び前記第2'信号を受信する受信部と、受信した前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数及び前記第3の換算定数を読取る処理と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化
5 処理と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2'信号を受け入れる認証をする認証処理と、を行う制御部と、を備える装置により実現できる。

また、本発明は、第1の換算定数、第2の換算定数、第3の換算定数及び第
10 4の換算定数のうち二の換算定数によって暗号化された送信データを含む第1'信号と第2'信号を受信して送信データを復号する装置であって、前記第1'信号には、前記第2の換算定数及び前記第4の換算定数を用いて前記送信データが暗号化された第1の代替値と、前記第1の換算定数と、前記第3の換算定数又は前記第4の換算定数と、が含まれ、前記第2'信号には、第1の換
15 算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第1の代替値と、第2の換算定数と、前記第1'信号に含まれていない第3の換算定数又は前記第4の換算定数と、が含まれ、前記第1'信号及び前記第2'信号を受信する受信部と、受信した前記第1'信号から前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は第4の換算定数、前記第2'
20 '信号から前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数又は第4の換算定数を読取る処理と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化処理と、前記第1の複合化データと前記第2の復号化データから前記第1'信号及び前記第2'信号を受け入れ
25 る認証をする認証処理と、を行う制御部を備える装置により実現できる。

また、本発明は、第1の換算定数、第2の換算定数及び第3の換算定数の

少なくとも一の換算定数によって暗号化された送信データを含む第1信号と第2信号を受信して送信データを復号化する装置であって、前記第1信号には、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第1の代替値と、第1の換算定数と、
5 が含まれ、前記第2信号には、前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第2の代替値と、前記第2の換算定数と、前記第3の換算定数に対応するパターン換算定数と、が含まれ、前記換算定数に対応するパターン換算定数を記憶する記憶部と、前記第1信号及び前記第2信号を受信する受信部と、前記第1
10 信号から前記第1の代替値、及び前記第1の換算定数、前記第2信号から前記第2の代替値、前記第2の換算定数、及び前記パターン換算定数を読取る処理と、前記読取られたパターン換算定数から前記第3の換算定数を取得する処理と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号
15 化する復号化処理と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証処理と、を行う制御部と、を備える装置により実現できる。

また、前記制御部は、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出するように構成することが
20 ことができる。

また、前記制御部は、前記第1の複合化データと前記第2の復号化データが一致したときに前記認証を行うように構成することができる。

図面の簡単な説明

25 図1は第1のデータ送信方法の説明図、図2は第2のデータ送信方法の説明図である。図3は実施例のデータ送信システムの説明図、図4は実施例のデ

一タ送受信側装置の構成図、図5は実施例の送信データの暗号化についての説明図、図6は実施例の第1信号の構成を表す説明図、図7は実施例の第2信号の構成を表す説明図である。

図8は実施例の送信側装置のパターン換算定数データの説明図、図9は実施例の中継装置のパターン換算定数データの説明図、図10は実施例の第2信号の構成を表す説明図、図11は実施例の送信信号の復号化についての説明図、図12は実施例の送信信号の復号化についてのデータ例を示す説明図、図13は実施例の送信側装置の処理の流れを示す説明図、図14は実施例の中継装置の処理の流れを示す説明図、図15及び図16は実施例の受信側装置の処理の流れを示す説明図である。

図17は第1のデータ送信方法の変形例を表す説明図、図18は第1のデータ送信方法の変形例を表す説明図である。図19は別実施例のデータ送信システムの説明図、図20は別実施例のデータ送信システムの構成装置の構成図、図21は別実施例の第1信号の構成を表す説明図、図22は別実施例の第2信号の構成を表す説明図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について図面を参照して説明する。なお、以下に説明する配置、形状等は、本発明を限定するものではなく、本発明の趣旨に沿って各種改変することができることは勿論である。

図1に基づき本発明のデータ送信システムに関する第1のデータ送信方法について説明する。本データ送信方法では、送信者(送信側装置)から受信者(受信側装置)へ、第1信号 S_1 と第2信号 S_2 が別々のルートで送信される。本発明の送信には、有線・無線回線を介した送信(例えば、赤外線通信、無線電波、光通信等による送信)及び伝送手段によるデータ等の送信(例えば、郵便等による配送)を含むものである。

まず、送信側装置では、暗号鍵となる換算定数 X 、 Y とパターン換算定数 Z が選択される。なお、送信側装置及び中継装置には、パターン換算定数 Z に対して換算定数 Z' が関連付けて登録されている。送信側装置及び中継装置では、パターン換算定数 Z が選択されると、これに対応して換算定数 Z' が読み出される。

送信側装置では、送信データ D は、換算定数 Y と Z' の組合せによって暗号化データ $D(Y, Z')$ に、換算定数 X と Z' の組合せによって暗号化データ $D(X, Z')$ に、それぞれ暗号化される。第1信号 S_1 には、暗号化データ $D(Y, Z')$ 、換算定数 X が含まれる。また、第2信号 S_2 には、暗号化データ $D(X, Z')$ 、換算定数 Y 、パターン換算定数 Z が含まれる。

第1信号 S_1 は、受信側装置へ送信される。一方、第2信号 S_2 は、一旦、中継装置に送信される。そして、第2信号 S_2 は、中継装置で第2'信号 S_2' に変換される。すなわち、中継装置では、受信された第2信号 S_2 に含まれるパターン換算定数 Z が換算定数 Z' に変換される。そして、第2'信号 S_2' は、中継装置から受信側装置へ送信される。なお、第1信号 S_1 及び第2信号 S_2 は、送信側装置から時間をずらして送信されるようにしてもよい。

受信側装置では、第1信号 S_1 及び第2'信号 S_2' を受信し、第1信号 S_1 から換算定数 X 、第2'信号 S_2' から換算定数 Y 、 Z' が読取られる。そして、第1信号 S_1 に含まれる暗号化データ $D(Y, Z')$ は、読取られた換算定数 Y と Z' の組合せによって復号化され、復号化データ D_1 が算出される。一方、第2'信号 S_2' に含まれる暗号化データ $D(X, Z')$ は、読取られた換算定数 X と Z' の組合せによって復号化され、復号化データ D_2 が算出される。

そして、復号化データ D_1 と D_2 との比較が行われる。受信側では両者が一致した場合に、復号化データ D_1 (又は D_2)を送信データ D として採用する。また、送信データ D には、受信側装置に接続された種々の外部駆動装置を駆動させるための駆動信号を含ませることができる。例えば、外部駆動装置としての口

ックシステムを開閉操作することが可能となる。

5 なお、上記暗号化例では、送信データDを換算定数YとZ'の組合せ及び換算定数X、Z'の組合せにより暗号化していたが、これに限らず、送信データDを換算定数YとZ'の組合せによる暗号化(D(Y, Z'))及び換算定数Xのみによる暗号化(D(X))をするようにしてもよい。この場合、第1信号S₁には暗号化データD(Y, Z')、換算定数Xが含まれ、第2信号S₂には暗号化データD(X)、換算定数Y、パターン換算定数Zが含まれる。

10 また、送信データDを換算定数Yのみによる暗号化(D(Y))、換算定数XとZ'による暗号化(D(X, Z'))をするようにし、第1信号S₁には暗号化データD(Y)、換算定数Xが含まれ、第2信号S₂には暗号化データD(X, Z')、換算定数Y、パターン換算定数Zが含まれるようにすることもできる。

15 このようにすれば、成りすまし送信された場合に、中継装置では不正な第2信号S₂に含まれるパターン換算定数Zが、登録された対応関係により換算定数Z'に変換される。そして、この対応関係が正しくない換算定数Z'を含む第2'信号S₂'が受信側へ転送される。

しかし、この換算定数Z'は成りすまし送信での暗号化に使用された換算定数とは異なるため、受信側で不正な第1信号S₁と不正な第2'信号S₂'をもとに復号化すると、得られる復号化データD₁とD₂が不一致となる。また、復号化データは、有意なデータとして復号することはできない。

20 以上のように第1のデータ送信方法では暗号化された送信データを2系統で送信する場合に、第1信号S₁に含まれる暗号化データの暗号鍵(換算定数Y)は第2信号S₂に含めて送信され、第2信号S₂に含まれる暗号化データの暗号鍵(換算定数X)は第1信号S₁に含めて送信される。

25 さらに、第1信号S₁及び第2信号S₂に含まれる暗号化データの共通の暗号鍵(換算定数Z')そのものは送付されず、暗号鍵に対応するパターン換算定数Zが第2信号S₂に含めて中継装置へ送信される。そして、このパターン換算

定数 Z が、中継装置で換算定数 Z' へ変換されることにより、第2信号 S_2 が第2'信号 S_2' に変換され、受信側へ転送される。

このように送信することにより、第3者は第1信号 S_1 及び第2信号 S_2 の双方を取得したとしてもパターン換算定数 Z が不明であるので、送信データ D の復号化を行うことはできない。また、第3者が第1信号 S_1 又は第2'信号 S_2' の一方を取得したとしても、それぞれの信号には換算定数のすべての換算定数が含まれていないので、復号化を行うことはできない。

さらに、第3者が第1信号 S_1 及び第2'信号 S_2' の双方を取得したとしても、復号化方法を取得しない限り、有意な復号化データを得ることはできない。

10 以上のように、第1のデータ送信方法では、第3者が暗号化データを不正に取得したとしても、暗号化データの復号化を有意に行うことができず、送信データの秘匿性を高めることができる。

また、受信側では、送信側で登録されたパターン換算定数を知らなくても暗号化データを復号化することができる。したがって、送信側では複数のパターン換算定数 Z 及び換算定数 Z' の組合せを登録することにより、複数の受信者(受信側装置)へ暗号化データを送信する場合にも秘匿性を高めることができる。

そして、第3者には換算定数 X 、 Y 、 Z' による暗号化方法及びパターン換算定数が不明であるため、送信者に成り代わって送信したとしても、受信側では有意なデータとして復号化することができない。または、復号化データが一致しない。これにより、成りすまし送信による不都合を回避することができる。

次に、図2に基づき第2のデータ送信方法について説明する。送信者(送信側装置)から受信者(受信側装置)へ第1信号 S_1 と第2信号 S_2 が別々のルートで送信されるのは、第1のデータ送信方法と同様である。また、送信側装置から送信される第1信号 S_1 及び第2信号 S_2 についても、暗号化方法やそれぞれに含められる換算定数等は同様である。

第2のデータ送信方法と上述の第1のデータ送信方法との違いは、第2信号 S_2 が中継装置を介して送信されないことである。そのため、第1のデータ送信方法では送信側と中継装置にパターン換算定数 Z 及び換算定数 Z' が登録されていたが、第2のデータ送信方法では送信側と受信側にパターン換算定数 Z 及び換算定数 Z' が登録されている。

したがって、受信側装置では、第1信号 S_1 及び第2信号 S_2 が受信され、第1信号 S_1 から換算定数 X 、第2信号 S_2 から換算定数 Y 及びパターン換算定数 Z が読取られる。そして、受信側装置で読取られたパターン換算定数 Z に対応する換算定数 Z' が読み込まれる。

これにより、第1信号 S_1 に含まれる暗号化データ $D(Y, Z')$ (又は $D(Y)$) は、換算定数 Y と Z' の組合せ (又は Y のみ) によって復号化データ D_1 に復号化され、第2信号 S_2 に含まれる暗号化データ $D(X, Z')$ (又は $D(X)$) は、換算定数 X と Z' の組合せ (又は X のみ) によって復号化データ D_2 に復号化される。

または、第1信号 S_1 に含まれる暗号化データ $D(Y, Z')$ (又は $D(Y)$) は、換算定数 Y と Z' の組合せ (又は Y) によって復号化データ D_1 に復号化され、第2信号 S_2 に含まれる暗号化データ $D(X)$ (又は $D(X, Z')$) は、換算定数 X (又は X と Z' の組合せ) によって復号化データ D_2 に復号化される。

そして、受信側では第1のデータ送信方法と同様に両者が一致した場合に、復号化データ D_1 (又は D_2) が送信データ D として採用される。

以上のように第2のデータ送信方法では暗号化された送信データを2系統で送信する場合に、第1信号 S_1 に含まれる暗号化データの暗号鍵 (換算定数 Y) は第2信号 S_2 に含めて送信され、第2信号 S_2 に含まれる暗号化データの暗号鍵 (換算定数 X) は第1信号 S_1 に含めて送信される。これは、第1のデータ送信方法と同様である。

そして、第1信号 S_1 及び第2信号 S_2 に含まれる暗号化データの共通の暗号鍵 (換算定数 Z') そのものは送付されず、暗号鍵に対応するパターン換算定

数 Z が第2信号 S_2 に含めて送信される。

そして、第2信号 S_2 を受信した受信側装置では、予め有しているパターン換
算定数 Z と換算定数 Z' の組合せの登録データを参照して、第2信号 S_2 に含ま
れるパターン換算定数 Z から換算定数 Z' を読み込み、さらに第1信号 S_1 及び
5 第2信号 S_2 から得られた換算定数 X , Y を使用して、送信データ D を復号化し
ている。

このように、送信側及び受信側に予めパターン換算定数を登録しておくこと
により、送信側と受信側との一対一の秘匿データ送信が可能となる。このよう
な、送信方法を利用して、例えば外部駆動装置としてのドアロックの開閉操作
10 等を行うことができる。漏洩データに対する復号化が困難であること、及び成り
すまし送信による不都合を回避できることは、第1のデータ送信方法と同様で
ある。

なお、第1及び第2の送信方法では、換算定数 X , Y , Z の3つの暗号鍵を用
いて暗号化しているが、換算定数 X , Y , Z は、それぞれ換算定数 X_1 , X_2 , \dots ,
15 換算定数 Y_1 , Y_2 , \dots , 換算定数 Z_1 , Z_2 , \dots , のようにそれぞれ複数の換算
定数を含む概念である。また、例えば、換算定数 X に複数の換算定数(X_1 , X_2 , \dots)
が用いられる場合は、これら複数の換算定数を第1信号 S_1 , 第2信号
 S_2 のどちらか、もしくは分散して両方に配置してもよい。

次に、第1の送信方法を用いた実施例の概略を図3に基づいて説明する。
20 本例のデータ送信システム S は、一方の送受信装置1(以下、「装置1」という)
からインターネット I を介して他方の送受信装置1へ暗号化された送信データを
送信するものである。

第1信号 S_1 は、送信側の装置1からプロバイダ P を介して受信側の装置1の
アドレスへ向けて送信され、受信側の装置1は第1信号 S_1 を受信する。また、
25 第2信号 S_2 は、送信側の装置1からプロバイダ P を介して中継配信サーバプロ
バイダ2(以下、「中継装置2」という)へ向けて送信される。中継装置2では、

第2信号 S_2 を第2'信号 S_2' に変換して、これを受信側の装置1のアドレスへ向けて送信する。受信側の装置1は、第2'信号 S_2' を受信する。

本例のデータ送信システムSでは、送信データとして個人認証番号A、搬送
認証番号B、制御データC、機密データDtが送信される。個人認証番号A、搬
5 送認証番号B、制御データCは、第1乃至第3の換算定数としての換算定数X、
Y、 Zy' で暗号化され、第1信号 S_1 及び第2信号 S_2 に含められる。また、機密
データDtは別途秘匿化されて第1信号 S_1 に含められる。

受信側の装置1では、第1信号 S_1 及び第2'信号 S_2' を受信して、両信号か
ら換算定数X、Y、 Zy' を読み取り、これらにより両信号に含まれる暗号化された
10 個人認証番号A、搬送認証番号B、制御データCに関するデータを復号し、ま
た、機密データDtの復号化を行う。さらに、復号化された制御データCに基づ
き、外部装置が駆動される。

本例の換算定数X、Yは、乱数によって装置1内で生成される。したがって、
送信毎に異なる換算定数が選択されるものである。また、送信側の装置1は、
15 特有のパターン換算定数データを有しており、パターン換算定数データには、
パターン換算定数 Zy と換算定数 Zy' の複数の組合せ(本例では、26通り)が
送信者により登録されている。なお、このパターン換算定数データは、中継装
置2にも送信者毎に対応して登録されている。

本システムSに登録された送信者は、固有の個人認証番号Aを有しており、
20 装置1を用いて個人認証番号A、搬送認証番号B、制御データC、機密データ
Dtを送信することができる。受信者は、送信者から送られてきた2つの信号を
受信し、これらから装置1によって送信データの認証を行い、個人認証番号A、
搬送認証番号B、制御データC、機密データDtを取得することができる。

搬送認証番号Bは、送信者が商品の搬送認証番号等を受信者に送付する
25 ためのものであり、売り手側から買い手側へ商品等を受け渡す流通手段とし
て、又は受け渡しロッカー等の用途に使用することができる。また、クレジットカ

ード番号の送信にも使用することができる。

制御データCは、送信側から受信側へ販売金額、利用回数、バーコード出力、リモート制御のON/OFF信号、鍵の解錠/施錠信号等の制御信号を送付するためのものである。

- 5 機密データDtは、送信者が受信者へ見積書、医療カルテ、法文書、成績書その他の機密文書等を封印して送信するためのものである。機密データDtは別途秘匿化されて第1信号S₁に含められる。

- 10 中継装置2には、上述のように複数の登録送信者ごとのパターン換算定数データが記憶されており、各登録送信者からの第2信号S₂を受信して、該信号中のパターン換算定数を該当する換算定数へ変換して第2'信号S₂'を生成し、第2信号S₂に付随して送信されてきた受信者のアドレスへ転送している。

- 15 また、中継装置2は、このようなデータ管理、データ変換及びデータ転送等の処理を行うと共に、データ転送等の処理に基づいて課金を行うための課金データ作成処理を行う。これにより、各登録送信者に対して、利用に応じて利用料の請求を行うことができる。このような課金については、利用回数、データ量等に応じて行うことが考えられる。

- 20 次に、図4に基づいて装置1及び中継装置2の構成について説明する。装置1は、専用機として構成してもよいが、通常のデスクトップ型のパソコンやモバイル端末を使用した構成としてもよい。装置1は、制御部としてのCPU100と、データの入出力を行うための入出力部101と、データの表示を行うための表示部102と、送受信部103と、各種データが記憶された記憶部110と、を備えている。

- 25 CPU100は、データの入出力制御、データ送受信制御、データの暗号化及び復号化処理、データ読取処理、第1信号及び第2信号の生成処理、認証処理、外部駆動装置の制御等を行う。データの暗号化処理については、CPU1

00は、乱数によって換算定数を自動選択(換算定数選択処理)し、該換算定数による所定の暗号化式にしたがって暗号化手段として入力データの暗号化(暗号化処理)を行う。なお、換算定数は送信者が指定して、該換算定数がCPU100に選択されるようにしてもよい。

- 5 入出力部101は、送信データとしての個人認証番号A、搬送認証番号B等や受信者のアドレス入力、パターン換算定数データ登録、データ暗号化・復号化処理、バーコードの読取処理等に用いられるものであり、例えばキーボード、マウス、バーコードリーダー、各種記憶メディアとのデータ入出力装置等から構成される。
- 10 表示部102は、入出力データ等の表示を行うものであり、例えばLCD装置等から構成される。送受信部103は、インターネットI及び外部駆動装置等に接続され、外部とデータの送受信を行うものであり、例えばモデムやLANカード等である。

- 記憶部110は、主記憶部111と、ROM112と、RAM113とを備える。主記憶部111には、オペレーティングシステムプログラムや、本例のデータ送受信処理等を行うためのプログラムを含む各種アプリケーションプログラム、パターン換算定数データ111a等が記憶されている。また、ROM112には、基本プログラム等が記憶され、ROM113は作業エリアとして用いられる。
- 15

- 送信者は、データ送信時にデータ送信システムS用の制御プログラムを起動して装置1の入出力部101から所定のデータの入力操作及びその他の送信操作を行う。また、受信者は、信号を受信して復号操作等を行う。
- 20

- また、本例の中継装置2は、プロパイダ内に配設されるサーバコンピュータとして実現することができる。中継装置2は、制御部としてのCPU200、入出力部201、表示部202、送受信部203、記憶部210とを備えている。記憶部210は、主記憶部211、ROM212、RAM213を備えている。また、主記憶部211内には、上述した登録者毎のパターン換算定数データ211aが記憶され
- 25

ている。CPU200は、信号の送受信処理、データ読取処理、信号の変換処理（信号生成処理）等を行う。

次に、図5に基づき送信データの暗号化について説明する。上述のように本例の暗号化には乱数によって生成される換算定数 X 、 Y 、及び送信者が選択
5 するパターン換算定数 Z_y に対応する換算定数 Z_y' が用いられる。なお、パターン換算定数 Z_y は送信者が選択するのではなく、暗号化時に登録されたパターン換算定数データから自動的に選択されるように構成してもよい。

図5に示すように、個人認証番号 A は第1式($A_x = A + Y + Z_y'$)及び第2式($A_y = A + X + Z_y'$)、搬送認証番号 B は第1式($B_x = B + Y + Z_y'$)及び第2式
10 ($B_y = B + X + Z_y'$)、制御データ C は第1式($C_x = C + Y + Z_y'$)及び第2式($C_y = C + X + Z_y'$)にしたがい暗号化される。それぞれのデータは、個人ID代替値(A_x , A_y)、搬送ID代替値(B_x , B_y)、制御データ代替値(C_x , C_y)に暗号化される。

例えば、図5に示したように、個人認証番号 A を「123456789012」、搬送
15 認証番号 B を「031234567890」、制御データ C を「20000」、換算定数 X を「223344」、換算定数 Y を「445566」、換算定数 Z を「3399」とすると、それぞれのデータは第1式及び第2式によって、個人認証番号 A は「123457237977」、「123457015755」、搬送認証番号 B は「031235016855」、「031234794633」、制御データ C は「468965」、「246743」に暗号化され
20 る。

本例の暗号化は、図5に示したように送信データに換算定数 X と Z_y' 、換算定数 Y と Z_y' がそれぞれ加算されるものであるが、これに限らず、減算、その他の演算方法であってもよい。また、上述したように送信データに換算定数 X と Z_y' 、換算定数 Y のみによって演算する方法、又は、送信データに換算定数 X のみ、換算定数 Y と Z_y' によって演算する方法により暗号化してもよい。
25

例えば、送信データに換算定数 X のみ、換算定数 Y と Z_y' による加算を行う場

合は、個人認証番号Aは第1式($A_x = A + Y + Z_y'$)及び第2式($A_y = A + X$)、
搬送認証番号Bは第1式($B_x = B + Y + Z_y'$)及び第2式($B_y = B + X$)、制御
データCは第1式($C_x = C + Y + Z_y'$)及び第2式($C_y = C + X$)にしたがい暗号
化される。このようにすると、より成りすまし送信に対する不都合を排除する効
5 果を向上させることができる。

次に、図6及び図7に基づき第1信号 S_1 及び第2信号 S_2 について説明する。
第1信号 S_1 及び第2信号 S_2 は、それぞれ大きさが指定されたパケット1乃至パ
ケット10の10のデータ領域からなる。パケット0は、第1信号 S_1 及び第2信号
 S_2 の内容を作成する際に入力するパスワードを一時的に格納するための領
10 域であって、実際にデータとしては送信されないものである。

パケット1は、通信番号格納領域であって送信信号に対して自動的に生起さ
れる番号である。パケット2は、送信者アドレス格納領域であって送信者の電
子メールアドレスが入力される。パケット3は、送信者の登録名の格納領域で
ある。
15 パケット4は、第1信号 S_1 の場合は換算定数Xが、第2信号 S_2 の場合は換算
定数Yが格納される領域である。パケット5は、パターン換算定数 Z_y の格納領
域である。本例の場合、パターン換算定数 Z_y は第1信号 S_1 には入力されず、
第2信号 S_2 のみに入力される。図7の例では、パターン換算定数 Z_y として「g」
が選択されている。パターン換算定数 Z_y の「g」は、換算定数Zの「3399」に対
20 応している。

パケット6は、第1信号 S_1 、第2信号 S_2 において、個人認証番号Aがそれぞ
れ第1式、第2式によって暗号化された個人ID代替値 A_x 、 A_y が格納される領
域である。同様にパケット7は、搬送認証番号Bがそれぞれ第1式、第2式によ
って暗号化された搬送ID代替値 B_x 、 B_y が格納される領域である。また、パケ
25 ット8は、制御データCがそれぞれ第1式、第2式によって暗号化された制御デ
ータ代替値 C_x 、 C_y が格納される領域である。

パケット9は、制御パターンCpが格納される領域である。制御パターンCpとは、制御データCの制御パターンを指定するものであり、例えば制御パターンCpがaの場合は、制御データCは回数を意味するものであることを表す。

同様に制御パターンCpが、b, c, d, eのときは、それぞれ制御データCは、プリペイド金額・販売金額等の金額データ、数値・バーコード出力等の数値データ、リモート制御のためのON/OFF信号データ、ロックシステムの解錠/施錠信号データを意味するものであることを表す。本例の場合、制御パターンCpは第1信号S₁のみに格納される。図6の例では、制御パターンCpとして「b」が選択されている。

また、パケット10は、機密データDtが格納される領域である。本例の場合、機密データDtは第1信号S₁のみに格納される。以上のような第1信号S₁及び第2信号S₂は、電子メールに添付されるデータファイルの形式で送信することができる。なお、制御パターンCp、機密データDtは、第2信号S₂に配置されてもよい。

図8に示すように、装置1内に記憶されるパターン換算定数データ111aは、パターン換算定数Z(a, b, ...)にそれぞれ対応して換算定数Zy'(1234, 2345, ...)が関係付けられたものである。登録送信者は、装置1に自らが指定した26の換算定数Zy'を登録することができる。また、データ送信システムSの管理者を介して、又は、直接、中継装置2に自ら指定したパターン換算定数データ111aを登録することができる。

図9に示すように、中継装置2内に登録されるパターン換算定数データ211aは、複数の登録送信者のパターン換算定数データ111aから構成されている。登録送信者ごとのパターン換算定数データ111aは、各登録送信者の電子メールアドレス及び送信者の登録名によって区別されている。

次に、図10に基づき第2'信号S₂'について説明する。送信側の装置1からの第2信号S₂は、プロバイダP経由で中継装置2へ一旦送信される。中継装

置2では、上述のように第2信号 S_2 から第2'信号 S_2' に変換される。

中継装置2では、第2信号 S_2 のパケット2(送信者アドレス)及びパケット3(登録名)を参照して、パターン換算定数データ211aから送信者のパターン換算定数データ111aが選択される。そして、選択されたパターン換算定数データ111aから第2信号 S_2 のパケット5(パターン換算定数 Z_y)を参照して、これ
5 に対応する換算定数 Z_y' が特定される。

換算定数 Z_y' が特定されると、第2信号 S_2 のパケット5が、特定されたパターン換算定数 Z_y' の値に変換された第2'信号 S_2' が生成される。このように、中継装置2では、受信された第2信号 S_2 が第2'信号 S_2' に変換される。そして、
10 第2'信号 S_2' は、送信者が指定する受信者の電子メールアドレスへ転送される。図10の例では、第2'信号 S_2' のパケット5(パターン換算定数格納領域)は「g」から「3399」へ変換される。

次に、図11に基づき受信側の装置1で行われる復号化処理の概略について説明する。受信側の装置1で第1信号 S_1 及び第2'信号 S_2' が受信されると、
15 両信号がペアリングされて仮認証される。このとき、通信番号、発信者アドレス等の一致が確認される。仮認証の結果、両信号が同一送信者からの受信信号であることが確認されると、両信号の暗号化データの復号化処理が行われる。

まず、復号化処理では、両信号から換算定数 X , Y , Z_y' が特定される。次に、
20 個人ID代替値を復号化するための第1式($A_1 = A_x - Y - Z_y'$)及び第2式($A_2 = A_y - Y - Z_y'$)によってそれぞれ第1信号 S_1 の個人ID代替値 A_x , 第2'信号 S_2' の個人ID代替値 A_y が復号化される。

そして、第1信号 S_1 及び第2'信号 S_2' のパケット3の送信者の登録名が一致すること、及び、復号化されたデータ(A_1 , A_2)が一致することが確認される。
25 登録名及び復号化データ A_1 と A_2 が一致すれば、両信号が最終的に認証される。

なお、個人ID代替値を復号化するための第1式が $A_1 = A_x - Y - Z_y'$ であり、第2式が $A_2 = A_y - Y$ である場合も同様に個人ID代替値 A_x 、 A_y が復号化されて復号化データ A_1 及び A_2 が算出され、登録名及び復号化データ A_1 及び A_2 の比較が行われ、両者が一致すれば、両信号が最終的に認証される。

- 5 また、最終的に認証されると、搬送ID代替値を復号化するための第1式($B_1 = B_x - Y - Z_y'$)及び第2式($B_2 = B_y - Y - Z_y'$)によってそれぞれ第1信号 S_1 の搬送ID代替値 B_x 、第2'信号 S_2' の搬送ID代替値 B_y が復号化され、復号化データ B_1 と B_2 が一致すれば、搬送認証番号 B として復号化データ B_1 (又は B_2)が採用される。
- 10 また、同様に、制御データ代替値を復号化するための第1式($C_1 = C_x - Y - Z_y'$)及び第2式($C_2 = C_y - Y - Z_y'$)によってそれぞれ第1信号 S_1 の制御データ代替値 C_x 、第2'信号 S_2' の制御データ代替値 C_y が復号化され、復号化データ C_1 と C_2 が一致すれば、制御データ C として復号化データ C_1 (又は C_2)が採用される。
- 15 搬送ID代替値を復号化するための第1式が $B_1 = B_x - Y - Z_y'$ 、第2式が $B_2 = B_y - Y$ であり、制御データ代替値を復号化するための第1式が $C_1 = C_x - Y - Z_y'$ 、第2式が $C_2 = C_y - Y - Z_y'$ である場合も同様である。
 また、制御パターン C_p により、制御データ C の種類が特定される。さらに、制御データ C の種類が、外部駆動装置へのON/OFF信号データ、解錠/施錠
 20 信号データであった場合は、受信側の装置1からさらに外部装置へ該信号が送出され、外部駆動装置が駆動されるようになっている。
- 25 図12に示すように、両信号の登録名が「xxxxxx」であるので、登録名(N_m)は一致する。そして、個人ID代替値 A_x として「123457237977」、個人ID代替値 A_y として「123457015755」を受信していた場合、換算定数 X 、 Y 、 Z_y'
 を所定のケットから読み出して復号化が行われると、図12の場合、復号化データ A_1 及び A_2 は共に「123456789012」となり両者は一致するため、両

信号は正規のものであるとの最終認証が行われる。

また、搬送ID代替値 B_x , B_y がそれぞれ「031235016855」, 「031234794633」であった場合は、復号化データ B_1 と B_2 が共に「031234567890」となるので両者は一致する。

- 5 また、制御データ代替値 C_x , C_y がそれぞれ「468965」, 「246743」であった場合は、復号化データ C_1 と C_2 が共に「20000」となるので両者は一致する。これにより、搬送認証番号 B , 制御データ C には、それぞれ「031234567890」, 「20000」が採用される。

次に、図13に基づき送信側の装置1のデータ処理の流れについて説明する。

- 10 まず、ステップS10では、画面表示に従って送信者が入力した所定のデータが読み込まれる。所定の入力データとしては、第1信号 S_1 及び第2信号 S_2 に関連したものとして、送信者の電子メールアドレス(パケット2), 送信者名(登録名、パケット3), パターン換算定数 Z_y (パケット5), 個人認証番号 A , 搬送認証番号 B , 制御データ C , 制御パターン C_p (パケット9), 機密データ D_t , また、
15 他のデータとして受信者の電子メールアドレス, 中継装置2の電子メールアドレス等がある。

なお、パスワード(パケット0)を入力するようにして、登録送信者以外の者が装置1を用いて送信操作できないように制限をかけるようにしてもよい。

- 20 次にステップS11では、データ入力(S10)されたタイミングで選択された2つの乱数(本例の場合6桁の数)を換算定数 X , Y とし、また、ステップS10で入力されたパターン換算定数 Z_y に対応する換算定数 Z_y' をパターン換算定数データ111aから読み出す。

- そして、ステップS12へ進み、ステップS10で入力された個人認証番号 A , 搬送認証番号 B , 制御データ C を換算定数 X , Y , Z_y' によって暗号化し、また、
25 別途機密データ D_t を暗号化する。機密データ D_t の暗号化手法については、個人認証番号 A , 制御データ C や換算定数 Z_y' 等を暗号鍵として暗号化してもよ

い。

ステップS13では、ステップS12で暗号化されたデータ及びステップS10で入力された入力データに基づき、所定の大きさを有する格納領域に各データを配置することにより第1信号 S_1 が生成される。

- 5 次にステップS14では、ステップS13と同様に第2信号 S_2 が生成される。ステップS13及びS14では、例えば第1信号 S_1 の packets 5のように配置すべきデータがない場合には、ブランクデータもしくは所定のスクランブルデータが配置される。

- 10 また、例えば搬送認証番号Bは送信するが、制御データCは送信する必要がない場合、制御データCにはステップS10でブランクデータが入力される。この場合も、ブランクデータ(又はスクランブルデータ)を入力データとして、ステップS13及びS14でデータが生成される。

- 15 そして、ステップS15では、送信者の送信入力に基づいて、先ず指定された受信者のアドレスへ第1信号 S_1 が送信される。次いでステップS16で、指定された中継装置2のアドレスへ第2信号 S_2 が送信され、処理を終了する。

次に、図14に基づき中継装置2での処理の流れについて説明する。中継装置2は、ステップS20で所定の電子メールアドレスに送信者からの第2信号 S_2 が送信されてくるのを待ち、ステップS20で第2信号 S_2 を受信すると(ステップS20;Yes)、ステップS21へ進み、送信者の識別を行う。

- 20 ステップS21では、受信した第2信号 S_2 の送信者の電子メールアドレス(パケット2)及び登録名(パケット3)を読み込む。そして、ステップS22で、該電子メールアドレス及び登録名がパターン換算定数データ211aに登録されているか否かを判別する。

- 25 ステップS22で該電子メールアドレス及び登録名が登録されていれば(ステップS22;Yes)、パターン換算定数データ211aを特定してステップS23へ進む。一方、登録されていなければ(ステップS22;No)、正規の登録送信者が

らの信号でないと判断して処理を終了する。なお、このとき、受信者へ不正な第2信号 S_2 を受信した旨の電子メールを送信するようにしてもよい。

ステップ23では、第2信号 S_2 のパターン換算定数 Z_y (パケット5)を読取る。ステップS24では、ステップS22で特定されたパターン換算定数データ111a
5 を参照して、読取られたパターン換算定数 Z_y に対応する換算定数 Z_y' を読取る。

そして、ステップS25で、ステップS24で読取られた換算定数 Z_y' を用いて第2'信号 S_2' を生成する。ステップS26では、ステップS25で生成された第2'信号 S_2' を、第2信号 S_2 と共に送付されてきた受信者の電子メールアドレスに送信し、処理を終了する。
10

次に、図15及び図16に基づき、受信側の装置1の処理の流れについて説明する。ステップS30で、第1信号 S_1 及び第2'信号 S_2' を受信して装置1内に取り込む。そして、装置1に取り込まれた第1信号 S_1 及び第2'信号 S_2' が受信者によって一対の信号であると指定される。具体的には、受信者が受取った電子メールに添付されたデータファイルが、装置1の画面上で第1信号 S_1 及び第2'信号 S_2' に指定される。
15

ステップS32では、指定された2つの信号の通信番号(パケット1)に相当するデータが比較される。両信号の通信番号が一致した場合は(ステップS32; Yes)、ステップS33へ進む。一方、両信号の通信番号が一致しなかった場合は(ステップS32; No)、ステップS48へ進み、表示部102にその旨のエラー表示をして処理を終了する。
20

ステップS33では、第1信号 S_1 のパケット3乃至パケット10のデータが読取られる。また、ステップS34では、第2'信号 S_2' のパケット3乃至パケット10のデータが読取られる。

25 次にステップS35では、個人ID代替値 A_x を復号化するための第1式から復号化データ A_1 が算出される。ステップS36では、個人ID代替値 A_y を復号化する

るための第2式から復号化データ A_2 が算出される。そして、ステップS37でステップS33及びS34で読取られた登録名、復号化データ A_1 と A_2 がそれぞれ比較され、一致するか否かが判別される。

5 これらが一致すると(ステップS37;Yes)、ステップS38へ進む。一方、一致しなかった場合は(ステップS37;No)、ステップS49へ進み、登録名、復号化データ A_1 と A_2 が一致しない旨のエラー表示をして処理を終了する。一致しない場合としては、成りすまし送信で暗号化式が不正であった場合、成りすまし送信でパターン換算定数 Z_y と換算定数 Z_y' との対応関係の不一致の場合等である。

10 ステップS38では、搬送ID代替値 B_x を復号化するための第1式から復号化データ B_1 が算出される。ステップS39では、搬送ID代替値 B_y を復号化するための第2式から復号化データ B_2 が算出される。そして、ステップS40で復号化データ B_1 と B_2 が比較され、一致するか否かが判別される。

15 これらが一致すると(ステップS40;Yes)、ステップS41へ進む。一方、一致しなかった場合は(ステップS40;No)、ステップS50へ進み、復号化データ B_1 と B_2 が一致しない旨のエラー表示をして処理を終了する。

ステップS41では、制御データ代替値 C_x を復号化するための第1式から復号化データ C_1 が算出される。ステップS42では、制御データ代替値 C_y を復号化するための第2式から復号化データ C_2 が算出される。そして、ステップS43

20 で復号化データ C_1 と C_2 が比較され、一致するか否かが判別される。

これらが一致すると(ステップS43;Yes)、ステップS44へ進む。一方、一致しなかった場合は(ステップS43;No)、ステップS51へ進み、復号化データ C_1 と C_2 が一致しない旨のエラー表示をして処理を終了する。

25 ステップS44では、機密データ D_t の復号がなされる。ステップS45では、復号化データ A_1 、 B_1 、 C_1 をそれぞれ、個人認証番号A、搬送認証番号B、制御データC、機密データ D_t として表示部102に表示する。また、制御パターン C_p

により、制御データCの種類が表示される。なお、機密データDtは、受信者によって手動で表示画面上において2つの受信信号が指定(例えば、両信号のデータファイルを重ね合わせる等)され、かつ復号データA₁とA₂が一致することを条件に、封印から開封(復号)されるように構成することができる。

- 5 ステップS46では、制御パターンCpにより制御データCが外部駆動装置を駆動する信号であるか否かが判別される。制御データCが外部駆動信号データであった場合は(ステップS46; Yes)、ステップS47へ進み、所定の外部駆動装置へ駆動信号を送出し、処理を終了する。一方、制御データCが外部駆動信号データでなかった場合は(ステップS46; No)、処理を終了する。
- 10 なお、上記実施例(第1のデータ送信方法)では、第1信号S₁はプロバイダPを介して直接、送信側の装置1から受信側の装置1へ送信されるが、第2信号S₂は中継装置2を介して第2'信号S₂'に変換されて受信側の装置1へ送信される。しかし、図17に示すように第2信号S₂だけでなく、第1信号S₁も別の中継装置2を介して受信側の装置1へ送信するようにしてもよい。
- 15 この場合、パターン換算定数データは、送信側の装置1及び2つの中継装置2に登録される。そして、送信側の装置1及び2つの中継装置2では、乱数により選択される換算定数X、Yと、パターン換算定数Z_x、Z_yを指定することによりそれぞれ特定される換算定数Z_x'、Z_y'の4つの換算定数が暗号鍵として用いられる。
- 20 送信側の装置1では、送信データDが換算定数Y、Z_y'により暗号化データD(Y, Z_y')に暗号化され(例えば、 $D(Y, Z_{y'}) = D + Y + Z_{y'}$)、また、換算定数X、Z_x'により暗号化データD(X, Z_x')に暗号化される(例えば、 $D(X, Z_{x'}) = D + X + Z_{x'}$)。
- 25 そして、第1信号S₁には、暗号化データD(Y, Z_y')、換算定数Xとパターン換算定数Z_xが含まれる。また、第2信号S₂には、暗号化データD(X, Z_x')、換算定数Yとパターン換算定数Z_yが含まれる。これら両信号は、送信側の

装置1からそれぞれ第1の中継装置2、第2の中継装置2へ送信される。

第1の中継装置2では、第1信号 S_1 のうちのパターン換算定数 Z_x が換算定数 Z_x' に変換されて第1'信号 S_1' が生成され、第1'信号 S_1' は受信側の装置1のアドレスへ転送される。また、第2の中継装置2では、第2信号 S_2 のうちの
5 パターン換算定数 Z_y が換算定数 Z_y' に変換されて第2'信号 S_2' が生成され、第2'信号 S_2' は受信側の装置1のアドレスへ転送される。

受信側の装置1では、第1'信号 S_1' から換算定数 X 、 Z_x が読取られ、第2'信号 S_2' から換算定数 Y 、 Z_y が読取られる。読取られた換算定数 X 、 Y 、 Z_x 、 Z_y によって、第1'信号 S_1' 及び第2'信号 S_2' は、それぞれ復号化データ D_1 及び
10 D_2 に復号化される。そして、受信側の装置1では、復号化データ D_1 と D_2 の比較認証が行われ、両者が一致すれば復号化データ D_1 (又は D_2)が送信データ D として採用される。

このように、2つの送信信号にそれぞれ異なる換算定数 Z_x 、 Z_y を用いて暗号化された暗号化データが含まれ、また、2つの送信信号には暗号化に用いられた換算定数ではない換算定数に対応するパターン換算定数が含められ、
15 2つの送信信号は、別々のルートを通して別々の中継装置2に一旦、送信され、中継装置2で送信信号に含まれたパターン換算定数が換算定数に変換され、それぞれ変換された送信信号が受信側の装置1に転送される。

20 このように、2ルート共に中継装置2を介して送信信号を変換・転送することにより、よりデータの秘匿性を高めることができ、成りすまし送信等の不正行為を確実に防止することができる。

また、上記実施例では、第1信号 S_1 及び第2信号 S_2 の双方がインターネットI経由で送信側から受信側へ送信されていたが、これに限らず、図18に示すように
25 一方向出力された第1信号 S_1 を搬送商品に添付して送付し、第2信号 S_2 は中継装置2を介してインターネットI経由で受信側へ送信する利用形態も

可能である。

第1信号 S_1 はバーコードリーダーによって受信側の装置1に取り込まれ、第2'信号 S_2' はインターネットI経由で受信される。これら両信号により搬送認証番号B等を復号化し、認証を行うことができる。

- 5 次に、図19に基づき第2のデータ送信方法による実施例を説明する。本実施例では、リモート制御により電子錠を解錠／施錠するロックシステムS-2に適用した例について説明する。本システムS-2は、第1信号 S_1 及び第2信号 S_2 を送信する装置3と、両信号を受信して外部駆動装置を駆動操作する装置4と、外部駆動装置としての電子錠5によって構成される。なお、第2のデータ
- 10 送信方法は、例えばパソコン等の個人認証に適用することも可能である。

- 装置3は、カード型の薄型小型装置であって、赤外線によって装置4へ第1信号 S_1 及び第2信号 S_2 を送信する。また、装置4は、赤外線受光部で該赤外線信号を受信して、該信号を認証後、外部駆動装置である電子錠5へ開閉駆動信号を送出する。電子錠5は、解錠／施錠駆動信号を受けるとこれに従い、
- 15 電子ロックの解錠又は施錠操作を行う。

図20に基づき本システムS-2の装置3及び装置4の構成を説明する。装置3は、制御部として機能するICチップであるCPU300と、操作パネルである入力部301と、データ送信伝送回路である送信部303と、LEDにより表示をおこなう表示部302と、記憶部310とを備える。

- 20 CPU300は、データの入出力、データ送信、換算定数選択処理、データの暗号化、信号生成処理等の制御を行う。入力部301は、テンキーと、例えば「OPN」(開)スイッチ、「CLS」(閉)スイッチ、登録スイッチ、送信スイッチのように、ある機能に特化されたスイッチや、その他の入力スイッチを有する。

- 表示部302は、CPU300の出力に従いLEDによる表示を行う。送信部30
- 25 3は、装置4へデータ信号の送信を行う信号発信素子を有する。記憶部310は、個人認証番号A、CPU300の制御プログラム、パターン換算定数データ3

10a等のデータが格納されており、また作業領域として機能するように構成されている。

なお、個人認証番号Aは送信者が有する認証カードに記憶され、装置3が個人認証番号Aを認証カードから接触又は非接触等の方式によって読取るよう

5 に構成してもよい。

装置4は、制御部であるCPU400と、操作パネル及び設定パネルを有する入力部401と、LCD表示器である表示部402と、装置3からのデータ信号を受信する受信部403と、記憶部410と、外部駆動装置とのインターフェース部404とを備える。

10 CPU400は、データの入出力制御、データ受信制御、データ読取処理、データの復号化、認証処理、外部駆動装置への駆動信号送出手の制御等を行う。入力部401は、各種入力スイッチから構成され、テンキー、アルファベットキー、特定の機能に特化したスイッチ(例えば、電源ON/OFFスイッチ、ドア開閉スイッチ等)等を有する。

15 表示部402は、CPU400からの出力に従い復号化データや、操作時の入力データ等の表示を行う。受信部403は、装置3からのデータ受信を行う受信ヘッドを有する。

記憶部410は、個人認証番号A、パターン換算定数データ410a、CPU400の制御プログラム等が記憶されており、またプログラムの作業領域として機能するように構成されている。パターン換算定数データ410aは装置3が有するパターン換算定数データ310aと同様のものである。なお、装置3からパターン換算定数データを装置4に送信して登録することができるようになっている。

装置3と装置4の間のデータ送信方式は、赤外線方式に限らず、無線電波方式、光通信方式、有線通信方式等が適用可能である。

25 外部駆動装置である電子錠5は、装置4のインターフェース部404と接続されており、装置4からの解錠駆動信号により電子ロックの解錠操作を行い、施

錠駆動信号により電子ロックの施錠操作を行う。また、外部駆動装置として電子錠5を複数接続することも可能である。

次に、図21及び図22に基づき、装置3から装置4へ送信される第1信号 S_1 及び第2信号 S_2 について説明する。上述の実施例と重複する部分については
5 説明を省略する。第1信号 S_1 及び第2信号 S_2 は、パケット0乃至4の5つのデータ領域を有する。パケット0は、通信番号格納領域である。パケット1は、換算定数 X 又は Y の格納領域である。パケット2は、パターン換算定数 Z_y の格納領域である。パターン換算定数 Z_y は、第2信号 S_2 のみに格納される。

パケット3は、個人ID代替値 A_x 又は A_y が格納される領域である。パケット4
10 は、解錠又は施錠を表すON/OFF信号格納領域である。信号としては、解錠を表す「1」、施錠を表す「0」がある。なお、複数の電子錠5を操作する場合は、各々の電子錠5を区別するためのパケット領域を設けるとよい。

該パケットに、各々の電子錠5に対して与えられた登録番号を格納し、該登録番号によって装置4から駆動信号を出力する電子錠5を区別するように構成
15 することができる。

換算定数 X 、 Y 、 Z_y' を用いて個人認証番号 A を暗号化する方法については、上述の実施例と同様である。なお、本例では、ON/OFF信号を暗号化することはしていないが、個人認証番号 A と同様に暗号化してもよい。また、パターン換算定数 Z_y 及び対応する換算定数 Z_y' の組合せデータは、装置3及び装置4
20 にそれぞれ登録されている。

次に本システムS-2の動作について説明する。送信者が、装置3の入力部301から解錠又は施錠データを入力(OPN(開)スイッチ又はCLS(閉)スイッチを押下)すると、表示部302にその旨が表示(「OPEN」又は「CLOSE」表示)される。次に、送信者はパターン換算定数 Z_y を指定するためのスイッチ操作をして(例えば、 Z_y = 「g」)、入力部301の送信スイッチを押下する。
25

CPU300は、送信スイッチが押下されたタイミングで乱数により換算定数 X 、

Yを選択し(例えば、 $X=1122$, $Y=3344$)、また、指定されたパターン換算定数 Z_y に対応する換算定数 Z_y' (例えば、 $Z_y'=3399$)を選択する。なお、換算定数 Z_y' はCPU300によって自動選択されるようにしてもよい。

次に、CPU300は、換算定数 X , Y , Z_y' によって個人認証番号 A を暗号化する。図20及び図21に示された例では、個人ID代替値 A_x は「12352421」($A_x=A+Y+Z_y'$)、個人ID代替値 A_y は「12350199」($A_y=A+X+Z_y'$)となる。そして、この暗号化データ等が組合せ配置され、第1信号 S_1 及び第2信号 S_2 が生成される。なお、個人認証番号 A を暗号化するための第1式を $A_x=A+Y+Z_y'$ とし、第2式を $A_y=A+X$ としてもよく、又、第1式を $A_x=A+Y$ とし、第2式を $A_y=A+X+Z_y'$ としてもよい。

第1信号 S_1 及び第2信号 S_2 が生成されると、CPU300は、該信号を送信部303から装置4の受信部403へ向けて、所定時間ずらしてそれぞれ送信する。このとき、それぞれの信号を複数回づつ送信してもよい。また、装置3及び装置4に送受信部を設け、装置3から装置4へ第1信号 S_1 が送信されると、装置4から装置3へアンサーバック信号が返信され、所定時間以内の該アンサーバック信号の受信を条件に装置3から装置4へ第2信号 S_2 が送信されるように構成してもよい。

装置4では、受信部403により第1信号 S_1 及び第2信号 S_2 が所定時間内に受信されると、該信号はCPU400によって読取られる。CPU400は、それぞれの信号の通信番号(パケット0)が一致するか否かを判別し、一致した場合は認証及び復号化処理へ移行する。しかし、通信番号は一致しなかった場合は、処理を終了する。このとき、通信番号が一致しなかった旨を音声により報知するようにしてもよい。なお、装置4への両信号の送信に先立ち、送信者のパスワードを装置4へ入力し、該パスワードが正しく認証されたことを条件として、装置4が両信号を受信可能とするように構成してもよい。

通信番号が一致すると、パターン換算定数データ410aを参照して、CPU4

00によって第2信号 S_2 のパターン換算定数 Z_y に対応する換算定数 Z_y' が読み込まれる。そして、個人ID代替値 A_x , A_y がそれぞれ換算定数 Y と Z_y' , 換算定数 X と Z_y' によって復号化される。そして、それぞれから得られた復号化データ A_1 ($A_1 = A_x - Y - Z_y'$) と A_2 ($A_2 = A_y - X - Z_y'$) が一致するか否かが判別
5 される。また、別の暗号化式では、復号化データ $A_1 = A_x - Y - Z_y'$, $A_2 = A_y - X$, 又は、復号化データ $A_1 = A_x - Y$, $A_2 = A_y - X - Z_y'$ となる。

両復号化データが一致した場合は、送信者が正規の送信者であると認証され、CPU400はON/OFF信号(パケット4)に基づいてインターフェース部404を介して、外部駆動装置(電子錠5)へ解錠/施錠駆動信号を送出する。一方、両復号化データが一致しなかった場合は、成りすまし者からの不正信号であると判別され、音声による報知がなされるように構成されている。
10

なお、両復号化データが一致しさらに、装置4が記憶している個人認証番号Aと復号化データが一致した場合に、送信者が正規の送信者であると認証されるようにしてもよい。このようにすることにより、さらに有効に成りすまし送信を排除することができる。
15

以上のように、装置3と装置4に共通のパターン換算定数データ310a及び410aが記憶されており、第1信号 S_1 及び第2信号 S_2 に含まれて送信される換算定数 X , Y 以外に、換算定数 Z_y' が暗号化に用いられている。したがって、仮に成りすまし送信信号が同様のデータ配置からなるものであったとしても、換算定数 X , Y 及び Z_y' による暗号化式、パターン換算定数 Z_y と換算定数 Z_y' との対応関係がわからない限り、装置4では不正な信号を受信したと判断される。
20

このように、本システムS-2では、成りすまし送信によっては装置4及び電子錠5は操作できないようになっているので、高い安全性を確保することが可能となる。
25

産業上の利用性

以上のように本発明によれば、第1のデータ送信方法として、送信側装置から送信データの送信が行われるとき、暗号化された送信データをそれぞれ含む第1信号と第2信号が設定され、それらは別々のルートで送信される。第1
5 信号には、第2の換算定数と第3の換算定数(又は第2の換算定数のみ)によって暗号化された送信データの代替値と、第1の換算定数と、が配置され送信される。一方、第2信号には、第1の換算定数と第3の換算定数(又は第1の換算定数のみ)によって暗号化された送信データの代替値と、第2の換算定数と、第3の換算定数と対応関係にあるパターン換算定数と、が配置され送
10 信される。

したがって、それぞれの信号が別ルートで送信されるので、安全性が確保されるのに加え、第1信号及び第2信号には、第3の換算定数自体は含まれておらず、仮に双方の信号が漏洩した場合であっても、第3者による送信データの復号化を行うことはできず、秘匿性が確保される。

15 そして、第2信号は中継装置へ一旦送信され、第2信号に含まれるパターン換算定数が対応する第3の換算定数に変換され、この信号は受信側装置へ転送される。したがって、送信側では、送信側装置にパターン換算定数と第3の換算定数との対応データを登録しておくと共に、中継装置にも同様のデータを登録しておけば、中継装置で第2信号を変換することができる。

20 このようにすることにより、送信データの秘匿性を確保できると共に、さらに複数のパターン換算定数を登録しておくことによりさらに秘匿性を高めることができる。また、受信側装置には、受信側装置のパターン換算定数を登録しておく必要がないので、送信側装置から複数の受信側装置に対して同一のパターン換算定数を使用して暗号化することも可能であり、暗号化に対する自由度が
25 高まる。

また、認証データの暗号化、復号化は、換算定数による容易なものであるに

も関わらず、安全なデータ送信が可能であり、データ送信に係る構成が簡単であるため、コストが掛からずにデータ送信システムを構築することができる。

また、本来の送信者になりかわって第3者がデータを送信したとしても、パターン換算定数及び第3の換算定数との対応関係がわからない限り、受信側装置では、両信号から送信データを復号したときに、有意なデータとして復号化
5 できないので、容易に成りすまし送信であることが判別できる。

また、受信側装置では、送信側装置からの第1信号と中継装置からの第2'信号を組み合わせることにより復号化が可能であるので、中継装置を介さずに第2'信号が送信されてきた場合にも、送信者アドレスからも成りすまし送信
10 であることを判別可能である。

また、第2のデータ送信方法として、中継装置を介さずに送信側装置から受信側装置へ第1信号及び第2信号が送信される場合にも、第1の換算定数、第2の換算定数及び第3の換算定数が用いられて送信データが暗号化され、第1及び第2の換算定数は第1信号又は第2信号に含められて送信されるが、
15 第3の換算定数自体は送信されず、その代わりに第3の換算定数に対応するパターン換算定数が送信信号に含められる。

そして、送信側装置及び受信側装置の双方にパターン換算定数を登録しておくことにより、受信側装置では、受信信号に含められたパターン換算定数に対応する第3の換算定数を知ることができ、第1信号及び第2信号から送信データ
20 を復号化することができる。

このようにすることにより、送信途中で第1信号及び第2信号が漏洩した場合であってもパターン換算定数に対応する第3の換算定数を知らない第3者は、送信データを復号化することができず秘匿性を確保することができる。

また、成りすまし送信された場合には、成りすまし送信の第2信号に含められたパターン換算定数と送信データを暗号化した第3の換算定数との関係が、
25 正規のパターン換算定数と第3の換算定数の関係に一致しないので、両信号

から復号化された復号化データが有意なデータとして復号化できないので、容易に成りすまし送信であることを判別可能である。

- 5 以上のように、本発明によれば、本来の送信者になりかわって第3者がデータを送信しても、受信者側で送信者の個人認証を行うことにより送信者を特定し、上記成りすまし送信による不都合を防ぐことができると共に、秘匿性の高いデータ送信システム及びデータ送信方法並びに装置を提供することができる。

請求の範囲

1. 送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、

- 5 前記送信側装置は、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択する換算定数選択手段と、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成手段と、前記第3の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号を前記受信側装置へ送信し前記第2信号を中継装置へ送信する送信手段と、を備え、
- 10

前記中継装置は、前記パターン換算定数に対応する第3の換算定数を記憶する記憶手段と、前記第2信号を受信して該第2信号に含まれるパターン換算定数を対応する前記第3の換算定数に変換して第2'信号を生成する信号生成手段と、前記第2'信号を前記受信側装置へ送信する送信手段と、を備え、

20 え、

- 前記受信側装置は、前記送信側装置からの前記第1信号及び前記中継装置からの第2'信号を受信して前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数及び前記第3の換算定数を読取る読取手段と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の複
- 25

合化データと前記第2の復号化データから前記第1信号及び前記第2'信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。

2. 送信側装置から受信側装置へ第1の換算定数、第2の換算定数、第3の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信システムであって、

前記送信側装置は、前記第1の換算定数、前記第2の換算定数、前記第3の換算定数及び前記第4の換算定数を選択する換算定数選択手段と、前記第2の換算定数及び前記第4の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第3の換算定数及び第4の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は前記第4の換算定数に対応するパターン換算定数を含む第1信号を生成する第1信号生成手段と、前記第2の代替値、前記第2の換算定数、及び前記第1信号に含まれない前記第3の換算定数又は前記第4の換算定数のパターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号を第1の中継装置へ送信し前記第2信号を第2の中継装置へ送信する送信手段と、を備え、

20 前記第1の中継装置は、前記パターン換算定数に対応する第3の換算定数又は第4の換算定数を記憶する記憶手段と、前記第1信号を受信して該信号に含まれるパターン換算定数を対応する前記第3の換算定数又は第4の換算定数に変換して第1'信号を生成する信号生成手段と、前記第1'信号を前記受信側装置へ送信する送信手段と、を備え、

25 前記第2の中継装置は、前記パターン換算定数に対応する第3の換算定数又は第4の換算定数を記憶する記憶手段と、前記第2信号を受信して該信号

に含まれるパターン換算定数を対応する前記第3の換算定数又は第4の換算定数に変換して第2'信号を生成する信号生成手段と、前記第2'信号を前記受信側装置へ送信する送信手段と、を備え、

前記受信側装置は、前記第1'信号及び前記第2'信号を受信して前記第1'信号から前記第1の代替値、前記第1の換算定数及び前記第3の換算定数又は第4の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数及び前記第3の換算定数又は第4の換算定数を読取る読取手段と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の複合化データと前記第2の復号化データから前記第1'信号及び前記第2'信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。

3. 送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信システムであって、

前記送信側装置は、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択する換算定数選択手段と、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化手段と、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成手段と、前記第3の換算定数に対応するパターン換算定数を記憶する記憶手段と、前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を含む第2信号を生成する第2信号生成手段と、前記第1信号及び前記第2信号を前記受信側装置へ送信する送信手段と、を備え、

前記受信側装置は、前記第1信号及び前記第2信号を受信して前記第1信

- 号から前記第1の代替値及び前記第1の換算定数、前記第2信号から前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を読取る読取手段と、前記パターン換算定数に対応する第3の換算定数を記憶する記憶手段と、前記読取られたパターン換算定数から前記第3の換算定数を読取る手段と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。
- 5 手段と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化手段と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証手段と、を備えたことを特徴とするデータ送信システム。
- 10 4. 前記暗号化手段は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化することを特徴とする請求項1又は3に記載のデータ送信システム。
5. 前記暗号化手段は、前記第2の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化することを特徴とする請求項1又は3に記載のデータ送信システム。
- 15 記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化することを特徴とする請求項1又は3に記載のデータ送信システム。
6. 前記暗号化手段は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数を用いて前記第2の代替値へ暗号化することを特徴とする請求項1又は3に記載のデータ送信システム。
- 20 用いて前記第2の代替値へ暗号化することを特徴とする請求項1又は3に記載のデータ送信システム。
7. 前記受信側装置は、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出手段を備えたことを特徴とする請求項1乃至3のいずれかに記載のデータ送信システム。
- 25 信システム。
8. 前記認証手段は、前記第1の複合化データと前記第2の復号化データが

一致したときに前記認証を行うことを特徴とする請求項1乃至3のいずれかに記載のデータ送信システム。

9. 前記送信側装置、前記中継装置及び前記受信側装置は、インターネットを含む通信回線網に接続されたことを特徴とする請求項1又は2に記載のデータ送信システム。

10. 前記送信側装置と受信側装置は、赤外線方式、無線電波方式、光通信方式、有線通信方式のいずれかによって前記信号の送受信を行うことを特徴とする請求項3に記載のデータ送信システム。

11. 送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、

前記送信側装置が、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択するステップと、

前記送信側装置が、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化ステップと、

前記送信側装置が、前記第1の代替値、及び前記第1の換算定数を含む第1信号を生成する第1信号生成ステップと、

20 前記送信側装置が、前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数に対応するパターン換算定数を含む第2信号を生成する第2信号生成ステップと、

前記送信側装置が、前記第1信号を前記受信側装置へ送信し前記第2信号を中継装置へ送信する第1送信ステップと、

25 前記中継装置が、前記第2信号を受信して該第2信号に含まれるパターン換算定数に対応する前記第3の換算定数に変換して第2'信号を生成する変

換ステップと、

前記中継装置が、前記第2'信号を前記受信側装置へ送信する第2送信ステップと、

5 前記受信側装置が、前記送信側装置からの前記第1信号及び前記中継装置からの第2'信号を受信して前記第1信号から前記第1の代替値、及び前記第1の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数を読取る読取ステップと、

10 前記受信側装置が、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化ステップと、

前記受信側装置が、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2'信号を受け入れる認証をする認証ステップと、を備えたことを特徴とするデータ送信方法。

12. 送信側装置から受信側装置へ第1の換算定数、第2の換算定数、第3
15 の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを送信するデータ送信方法であって、

前記送信側装置が、前記第1の換算定数、前記第2の換算定数、前記第3の換算定数及び前記第4の換算定数を選択するステップと、

20 前記送信側装置が、前記第2の換算定数、及び前記第4の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化ステップと、

前記送信側装置が、前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は前記第4の換算定数に対応するパターン換算定数を含む
25 第1信号を生成する第1信号生成ステップと、

前記送信側装置が、前記第2の代替値、前記第2の換算定数、及び前記第

1 信号に含まれない前記第3の換算定数又は前記第4の換算定数のパターン換算定数を含む第2信号を生成する第2信号生成ステップと、

前記送信側装置が、前記第1信号を第1の中継装置へ送信し前記第2信号を第2の中継装置へ送信する第1送信ステップと、

- 5 前記第1の中継装置及び前記第2の中継装置が、前記第1信号又は前記第2信号を受信して該信号に含まれるパターン換算定数に対応する前記第3の換算定数又は第4の換算定数に変換して第1'信号又は第2'信号を生成する変換ステップと、

- 10 前記第1の中継装置及び前記第2の中継装置が、前記第1'信号又は前記第2'信号を前記受信側装置へ送信する第2送信ステップと、

- 前記受信側装置が、前記第1'信号及び前記第2'信号を受信して前記第1'信号から前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は第4の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数又は第4の換算定数を読み取る読み取りステップと、
- 15

前記受信側装置が、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化ステップと、

- 20 前記受信側装置が、前記第1の複合化データと前記第2の復号化データから前記第1'信号及び前記第2'信号を受け入れる認証をする認証ステップと、を備えたことを特徴とするデータ送信方法。

13. 送信側装置から受信側装置へ第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信するデータ送信方法であって、

- 25 前記送信側装置が、前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択するステップと、

前記送信側装置が、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化ステップと、

- 5 前記送信側装置が、前記第1の代替値及び前記第1の換算定数を含む第1信号を生成する第1信号生成ステップと、

前記送信側装置が、前記第2の代替値、前記第2の換算定数及び前記第3の換算定数に対応するパターン換算定数を含む第2信号を生成する第2信号生成ステップと、

- 10 前記送信側装置が、前記第1信号及び前記第2信号を前記受信側装置へ送信する送信ステップと、

前記受信側装置が、前記第1信号及び前記第2信号を受信して前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2信号から前記第2の代替値、前記第2の換算定数及び前記パターン換算定数を読取る読

- 15 取ステップと、

前記受信側装置が、前記読取られたパターン換算定数に対応する前記第3の換算定数を取得する換算定数取得ステップと、

前記受信側装置が、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化

- 20 データへ復号化する復号化ステップと、

前記受信側装置が、前記第1の復号化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証ステップと、を備えたことを特徴とするデータ送信方法。

14. 前記暗号化ステップでは、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化することを
- 25

特徴とする請求項11又は13に記載のデータ送信方法。

15. 前記暗号化ステップでは、前記第2の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化することを特徴とする請求項11又は13に記載のデータ送信方法。
16. 前記暗号化ステップでは、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数を用いて前記第2の代替値へ暗号化することを特徴とする請求項11又は13に記載のデータ送信方法。
- 10 17. 前記認証ステップの後、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出する駆動信号送出ステップを備えたことを特徴とする請求項11乃至13のいずれかに記載のデータ送信方法。
- 15 18. 前記認証ステップでは、前記第1の複合化データと前記第2の復号化データが一致したときに前記認証を行うことを特徴とする請求項11乃至13のいずれかに記載のデータ送信方法。
19. 第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを送信する装置であって、
前記換算定数に対応するパターン換算定数を記憶する記憶部と、
- 20 前記第1の換算定数、前記第2の換算定数及び前記第3の換算定数を選択する換算定数選択処理と、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の代替値へ暗号化する暗号化処理と、前記第1
- 25 の代替値、及び前記第1の換算定数を含む第1信号を生成する第1信号生成処理と、前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数

に対応するパターン換算定数を含む第2信号を生成する第2信号生成処理と、前記第1信号と前記第2信号をそれぞれ送信する処理と、を行う制御部と、

前記第1信号と前記第2信号を外部へ送信する送信部と、を備えたことを特徴とする装置。

- 5 20. 前記制御部は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化することを特徴とする請求項19に記載の装置。

- 10 21. 前記制御部は、前記第2の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数及び前記第3の換算定数を用いて前記第2の代替値へ暗号化することを特徴とする請求項19に記載の装置。

- 15 22. 前記制御部は、前記第2の換算定数及び前記第3の換算定数を用いて前記送信データを前記第1の代替値へ暗号化し、前記第1の換算定数を用いて前記第2の代替値へ暗号化することを特徴とする請求項19に記載の装置。

23. 第1の換算定数、第2の換算定数、第3の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを送信する装置であって、

- 20 前記換算定数に対応するパターン換算定数を記憶する記憶部と、
前記第1の換算定数、前記第2の換算定数、前記第3の換算定数及び前記第4の換算定数を選択する換算定数選択処理と、前記第2の換算定数及び前記第4の換算定数を用いて前記送信データを第1の代替値に暗号化し前記第1の換算定数及び前記第3の換算定数を用いて前記送信データを第2の
25 代替値へ暗号化する暗号化処理と、前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は前記第4の換算定数に対応するパターン換

算定数を含む第1信号を生成する第1信号生成処理と、前記第2の代替値、前記第2の換算定数、及び前記第1信号に含まれない前記第3の換算定数又は前記第4の換算定数のパターン換算定数を含む第2信号を生成する第2信号生成処理と、を行う制御部と、

- 5 前記第1信号と前記第2信号を外部へ送信する送信部と、を備えたことを特徴とする装置。

24. 送信データの暗号化に用いられる換算定数に対応するパターン換算定数を含む信号を転送する装置であって、

前記換算定数に対応するパターン換算定数を記憶する記憶部と、

- 10 前記信号を送受信する送受信部と、

受信した前記信号に含まれるパターン換算定数に対応する前記換算定数に変換して前記信号を変換する信号生成処理と、前記変換された信号を転送する処理と、を行う制御部と、を備えたことを特徴とする装置。

25. 第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第1信号と第2'信号を受信して送信データを復号化する装置であって、

前記第1信号には、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第1の代替値と、第1の換算定数と、が含まれ、

- 20 前記第2'信号には、前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第2の代替値と、前記第2の換算定数と、前記第3の換算定数と、が含まれ、

前記第1信号及び前記第2'信号を受信する受信部と、

- 25 受信した前記第1信号から前記第1の代替値及び前記第1の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数及び前記第3の換算定数を読取る処理と、前記第1の代替値及び前記第2の代替値をそれぞれ

暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化処理と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2'信号を受け入れる認証をする認証処理と、を行う制御部と、を備えたことを特徴とする装置。

- 5 26. 第1の換算定数、第2の換算定数、第3の換算定数及び第4の換算定数のうち二の換算定数によって暗号化された送信データを含む第1'信号と第2'信号を受信して送信データを復号する装置であって、

- 前記第1'信号には、前記第2の換算定数及び前記第4の換算定数を用いて前記送信データが暗号化された第1の代替値と、前記第1の換算定数と、
10 前記第3の換算定数又は前記第4の換算定数と、が含まれ、

前記第2'信号には、第1の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第1の代替値と、第2の換算定数と、前記第1'信号に含まれていない第3の換算定数又は前記第4の換算定数と、が含まれ、

- 15 前記第1'信号及び前記第2'信号を受信する受信部と、

- 受信した前記第1'信号から前記第1の代替値、前記第1の換算定数、及び前記第3の換算定数又は第4の換算定数、前記第2'信号から前記第2の代替値、前記第2の換算定数、及び前記第3の換算定数又は第4の換算定数を読取る処理と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に
20 用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化処理と、前記第1の複合化データと前記第2の復号化データから前記第1'信号及び前記第2'信号を受け入れる認証をする認証処理と、を行う制御部を備えたことを特徴とする装置。

27. 第1の換算定数、第2の換算定数及び第3の換算定数の少なくとも一の換算定数によって暗号化された送信データを含む第1信号と第2信号を受
25 信して送信データを復号化する装置であって、

前記第1信号には、前記第2の換算定数、又は前記第2の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第1の代替値と、第1の換算定数と、が含まれ、

5 前記第2信号には、前記第1の換算定数、又は前記第1の換算定数及び前記第3の換算定数を用いて前記送信データが暗号化された第2の代替値と、前記第2の換算定数と、前記第3の換算定数に対応するパターン換算定数と、が含まれ、

前記換算定数に対応するパターン換算定数を記憶する記憶部と、

前記第1信号及び前記第2信号を受信する受信部と、

10 前記第1信号から前記第1の代替値、及び前記第1の換算定数、前記第2信号から前記第2の代替値、前記第2の換算定数、及び前記パターン換算定数を読取る処理と、前記読取られたパターン換算定数から前記第3の換算定数を取得する処理と、前記第1の代替値及び前記第2の代替値をそれぞれ暗号化に用いられた換算定数によって第1の復号化データ及び第2の復号化データへ復号化する復号化処理と、前記第1の複合化データと前記第2の復号化データから前記第1信号及び前記第2信号を受け入れる認証をする認証処理と、を行う制御部と、を備えたことを特徴とする装置。

28. 前記制御部は、前記第1の復号化データ又は第2の復号化データに基づき、外部駆動装置を駆動するための駆動信号を送出することを特徴とする
20 請求項25乃至27のいずれかに記載の装置。

29. 前記制御部は、前記第1の複合化データと前記第2の復号化データが一致したときに前記認証を行うことを特徴とする請求項25乃至27のいずれかに記載の装置。

図 1

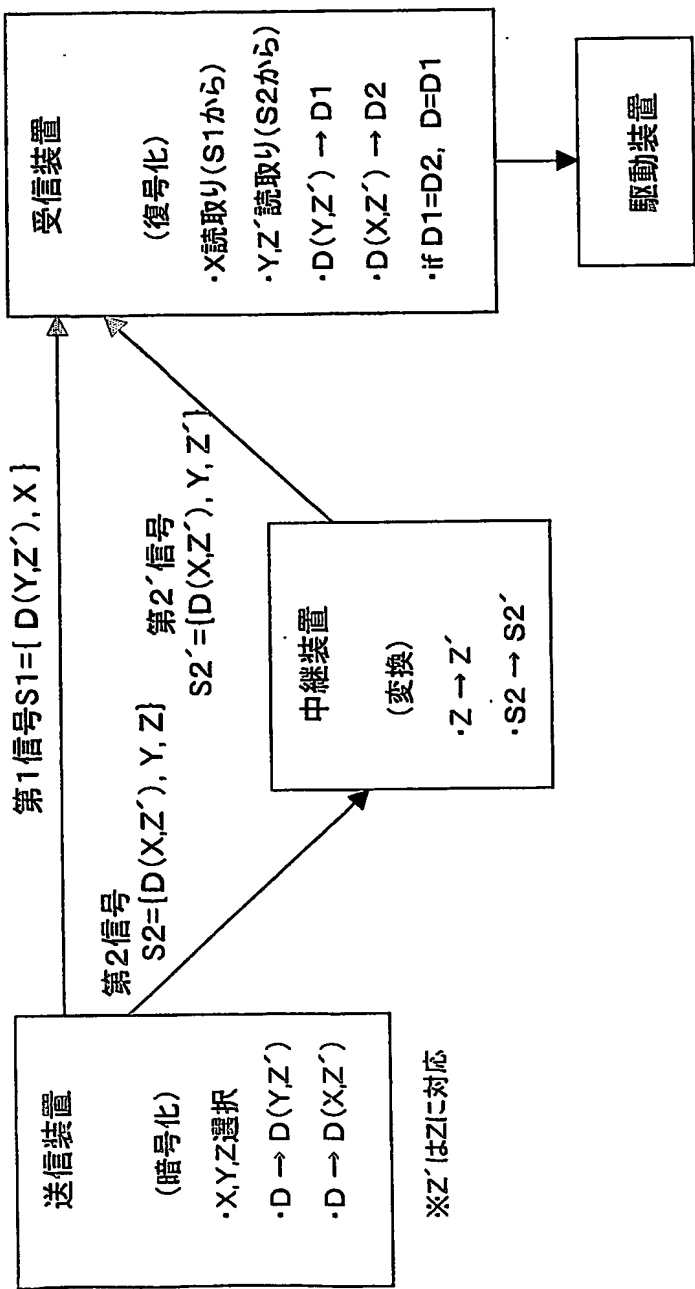


図 2

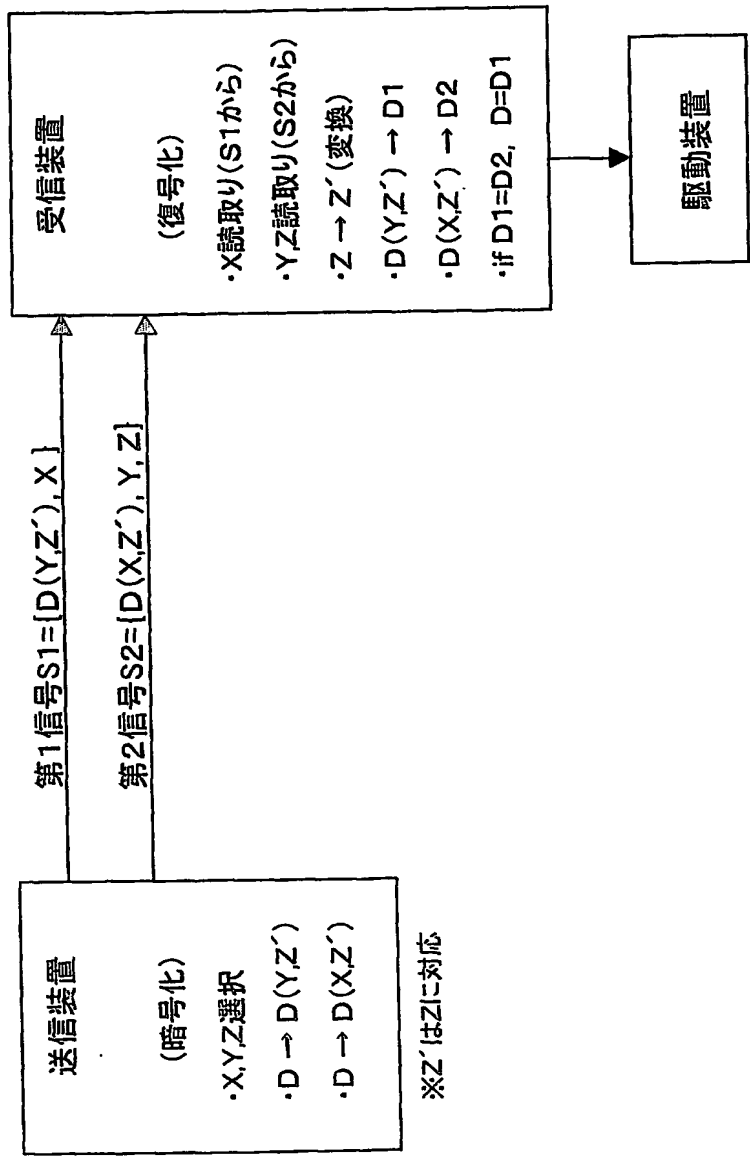
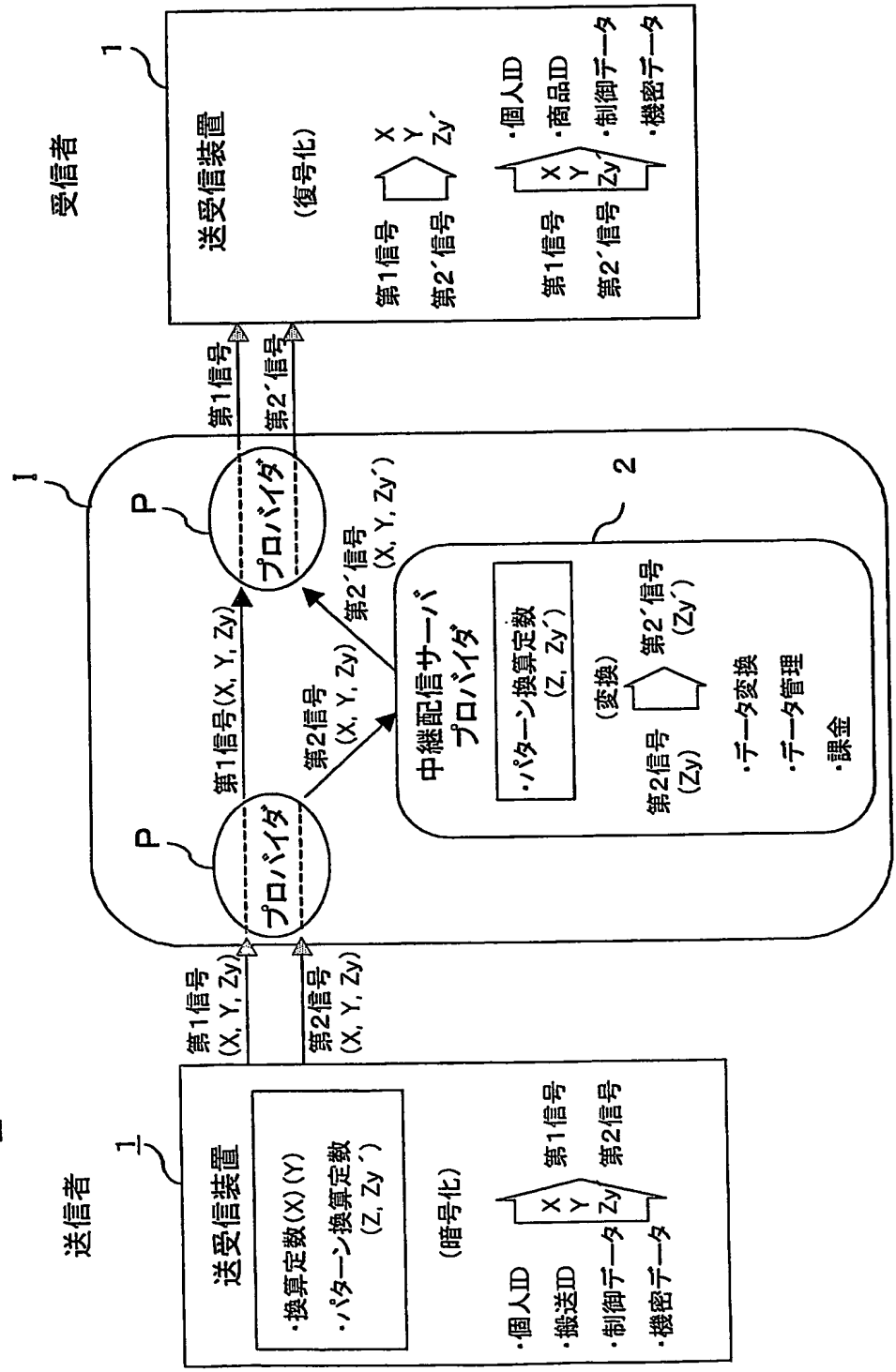


図 3



4 / 19

図 4

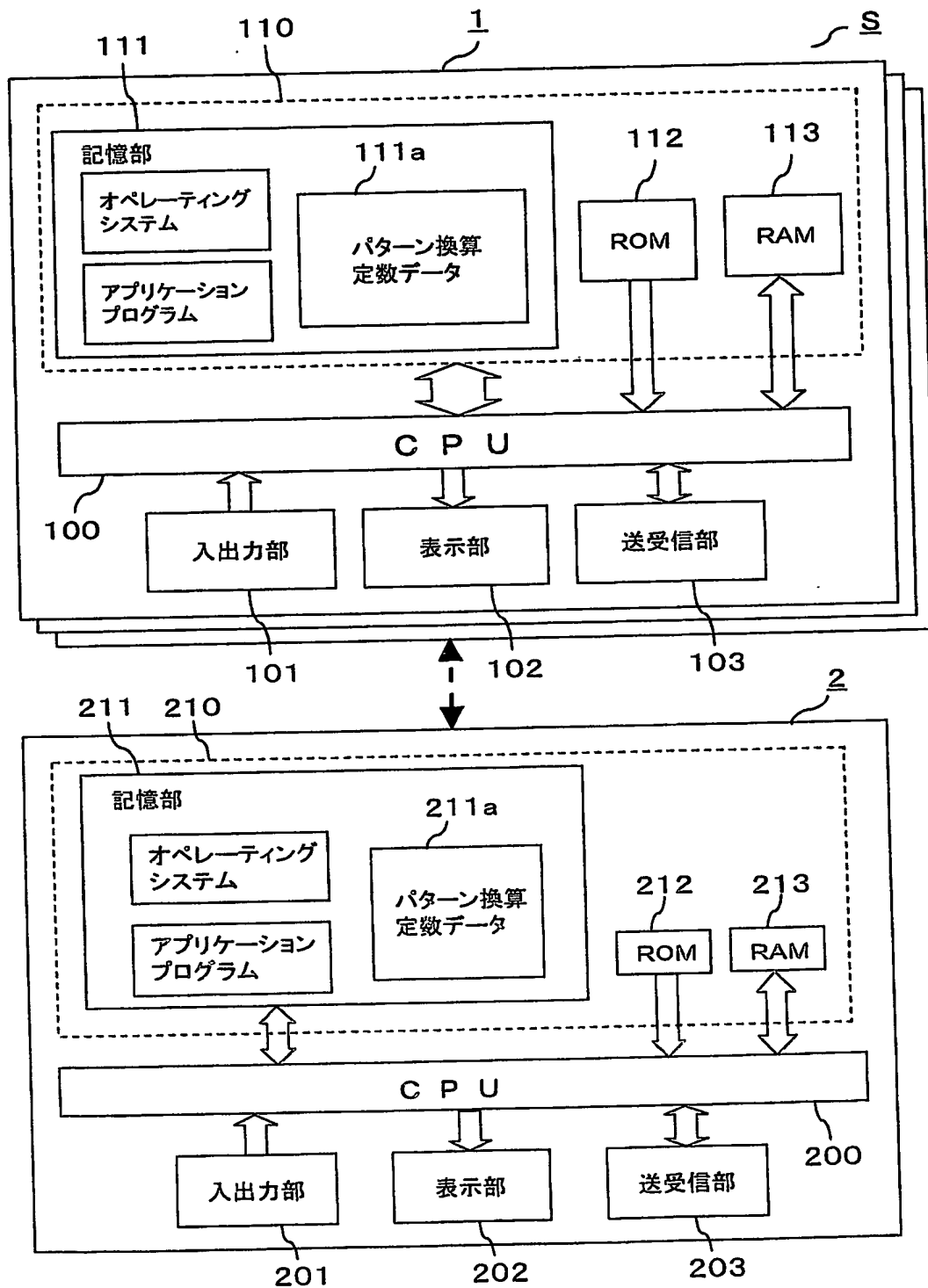


図 5

| 信号暗号化 A(個人認証番号):1234 5678 9012 B(搬送認証番号):0312 3456 7890 C(制御データ):20000 | | | |
|--|--------------------------|----------------|--|
| 暗号化データ | 復号式 | 信号暗号化データ例 | |
| A個人IDデータ | 第1式 $A_x = A + Y + Z_y'$ | 1234 5723 7977 | $= (1234\ 5678\ 9012) + (44\ 5566) + (3399)$ |
| | 第2式 $A_y = A + X + Z_y'$ | 1234 5701 5755 | $= (1234\ 5678\ 9012) + (22\ 3344) + (3399)$ |
| B搬送IDデータ | 第1式 $B_x = B + Y + Z_y'$ | 0312 3501 6855 | $= (0312\ 3456\ 7890) + (44\ 5566) + (3399)$ |
| | 第2式 $B_y = B + X + Z_y'$ | 0312 3479 4633 | $= (0312\ 3456\ 7890) + (22\ 3344) + (3399)$ |
| C制御データ | 第1式 $C_x = C + Y + Z_y'$ | 46 8965 | $= (2\ 0000) + (44\ 5566) + (3399)$ |
| | 第2式 $C_y = C + X + Z_y'$ | 24 6743 | $= (2\ 0000) + (22\ 3344) + (3399)$ |

X, Y, Z_{y'}:換算定数

図 6

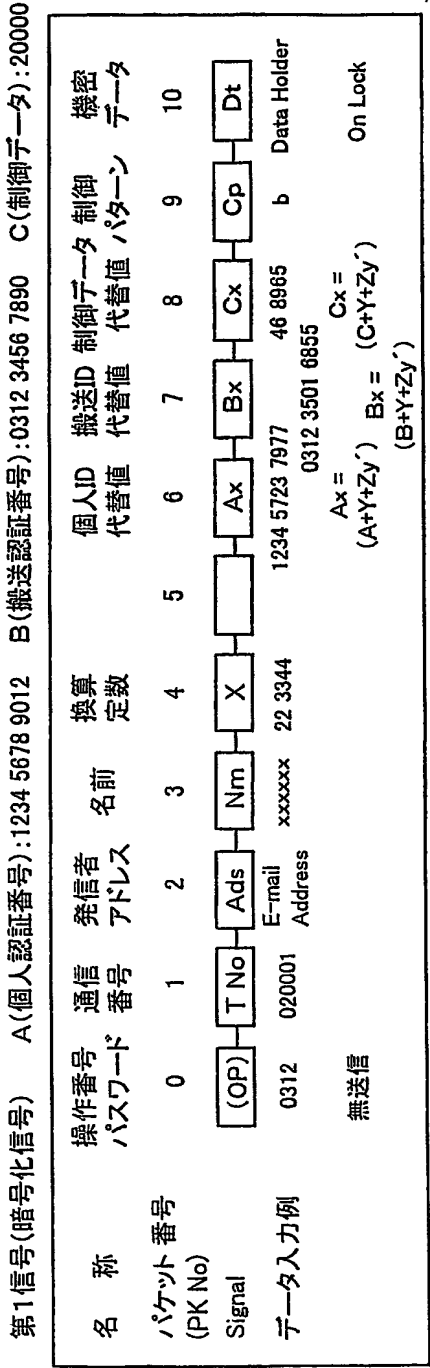


図 7

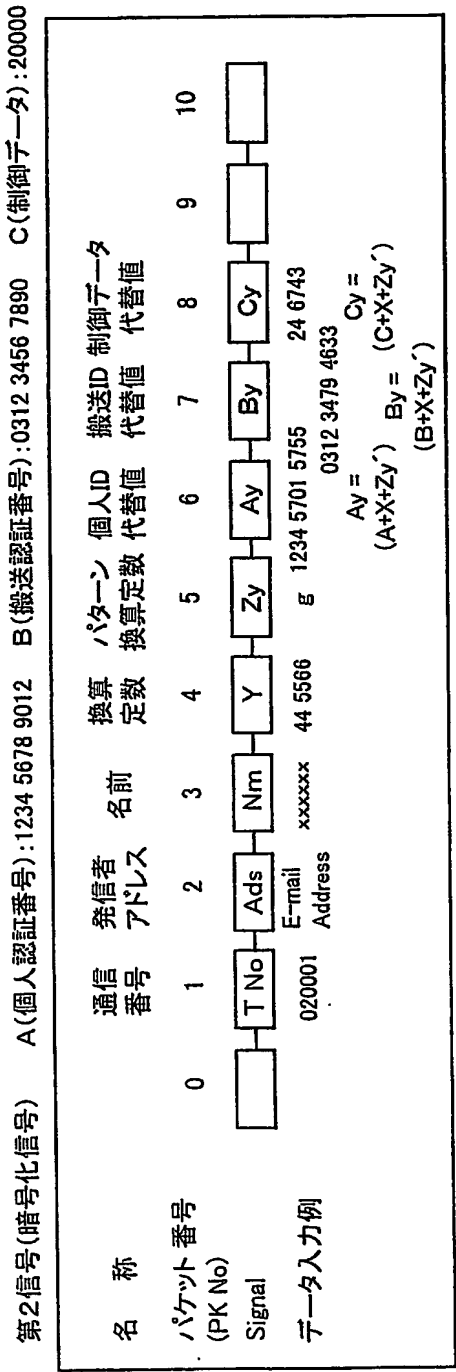


図 8

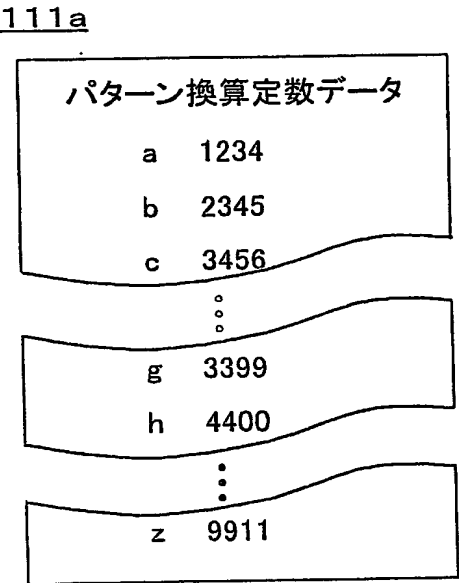


図 9

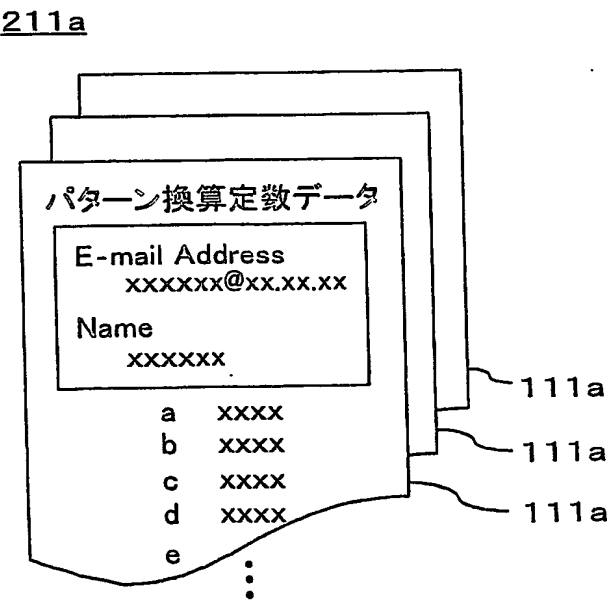
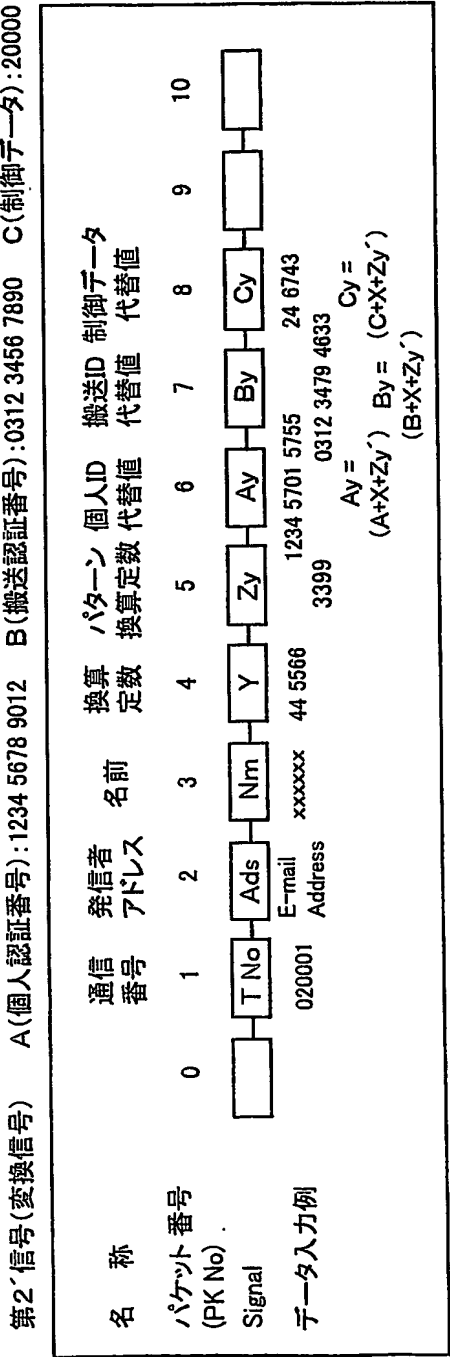


図 10



10/19

図 11

信号復号化

| 復号化データ | 復号式 | 認証 |
|----------|------------------------------|-------|
| A個人IDデータ | 第1式 $Nm / Ax - Y - Zy' = A1$ | A1=A2 |
| | 第2式 $Nm / Ay - X - Zy' = A2$ | |
| B搬送IDデータ | 第1式 $Bx - Y - Zy' = B1$ | B1=B2 |
| | 第2式 $By - X - Zy' = B2$ | |
| C制御データ | 第1式 $Cx - Y - Zy' = C1$ | C1=C2 |
| | 第2式 $Cy - X - Zy' = C2$ | |

1 1 / 1 9

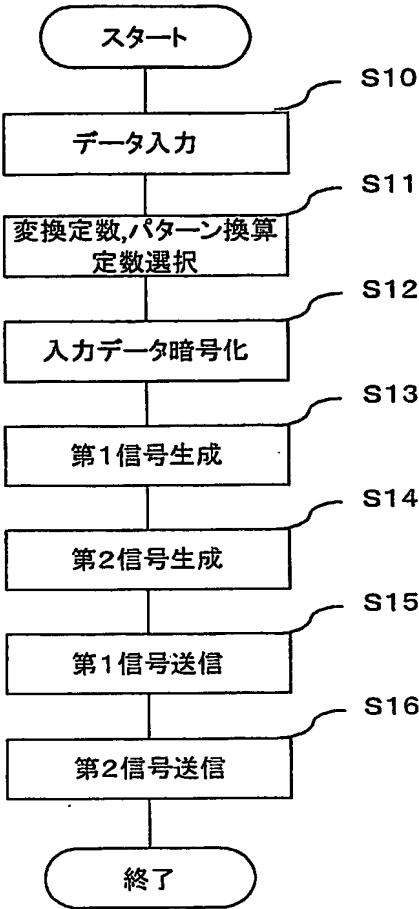
図 1 2

信号復号化データ例 A(個人認証番号):1234 5678 9012 B(搬送認証番号):0312 3456 7890 C(制御データ):20000

| | | | |
|----------|--|----------------|----|
| A個人IDデータ | Nm 第1式 (xxxxxx)/(1234 5723 7977)-(44 5566)-(3399) = xxxxxx/1234 5678 9012 | Ax Y Zy' | A1 |
| | Nm 第2式 (xxxxxx)/(1234 5701 5755)-(22 3344)-(3399) = xxxxxx/1234 5678 9012 | Ay X Zy' | A2 |
| B搬送IDデータ | Bx 第1式 (0312 3501 6855)-(44 5566)-(3399) = 0312 3456 7890 | Y Zy' | B1 |
| | By 第2式 (0312 3479 4633)-(22 3344)-(3399) = 0312 3456 7890 | X Zy' | B2 |
| C制御データ | Cx 第1式 (46 8965)-(44 5566)-(3399) = 2 0000 (¥20,000) | Y Zy' | C1 |
| | Cy 第2式 (24 6743)-(22 3344)-(3399) = 2 0000 (¥20,000) | X Zy' | C2 |

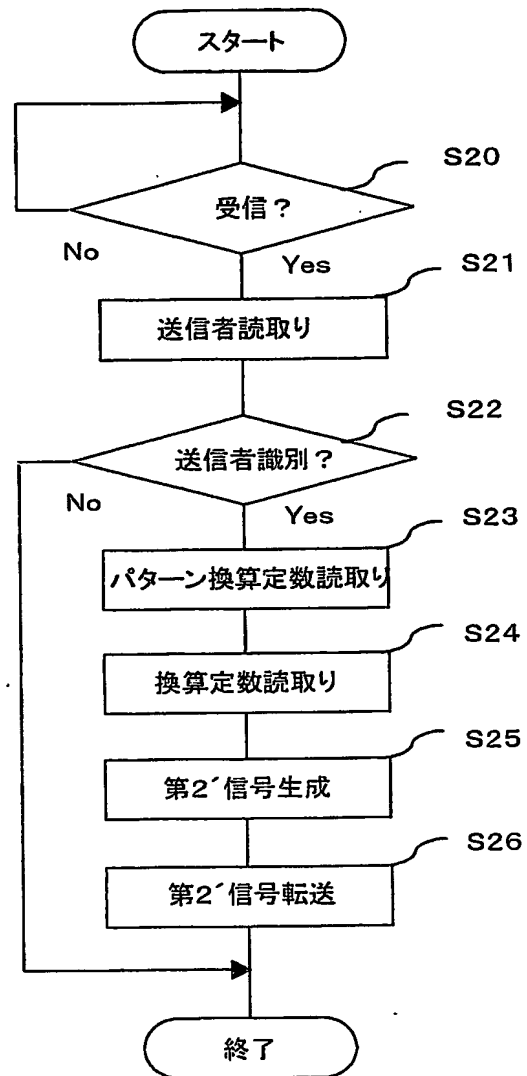
12/19

図 13



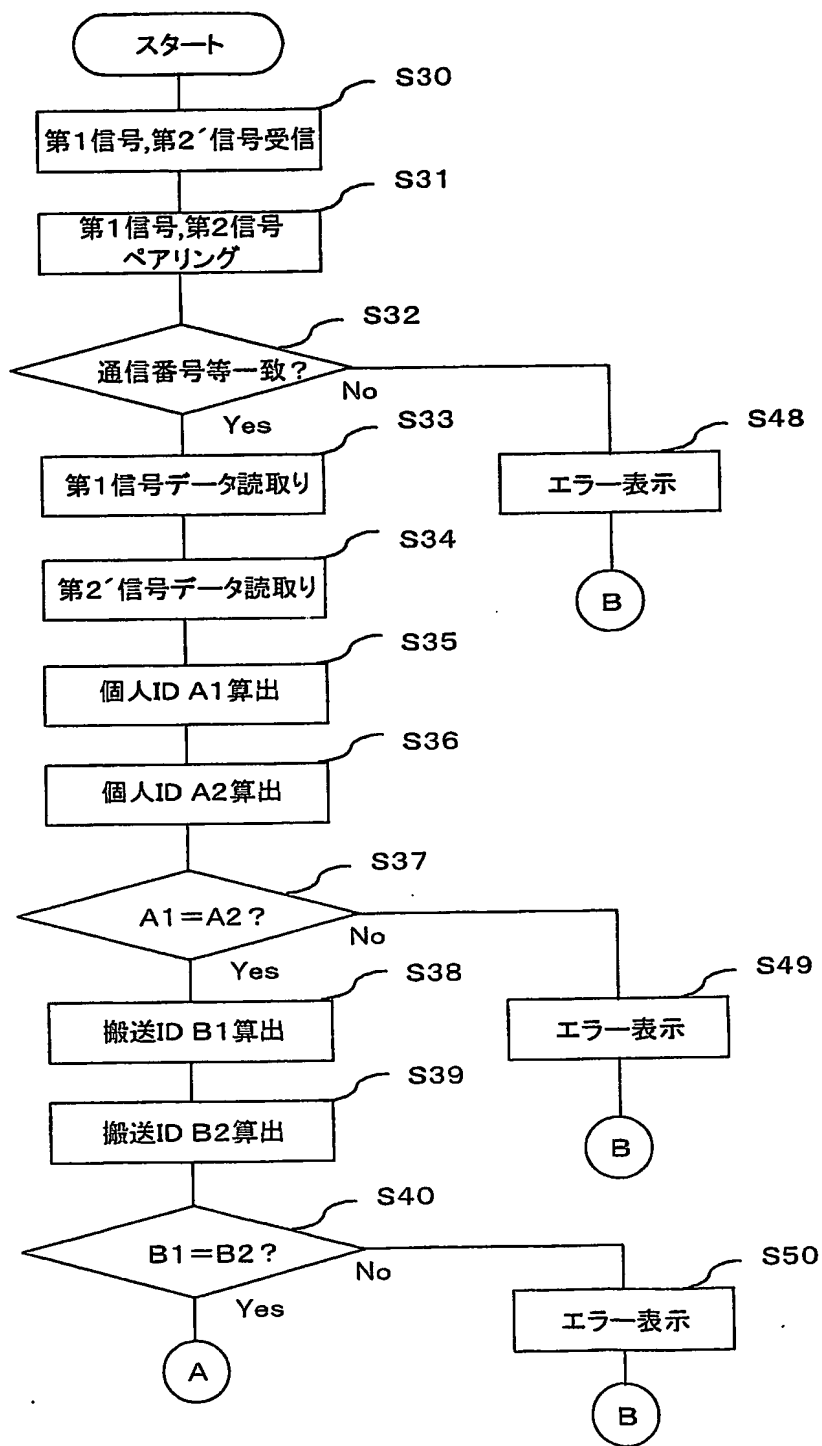
13/19

図 14



14/19

図 15



15 / 19

図 16

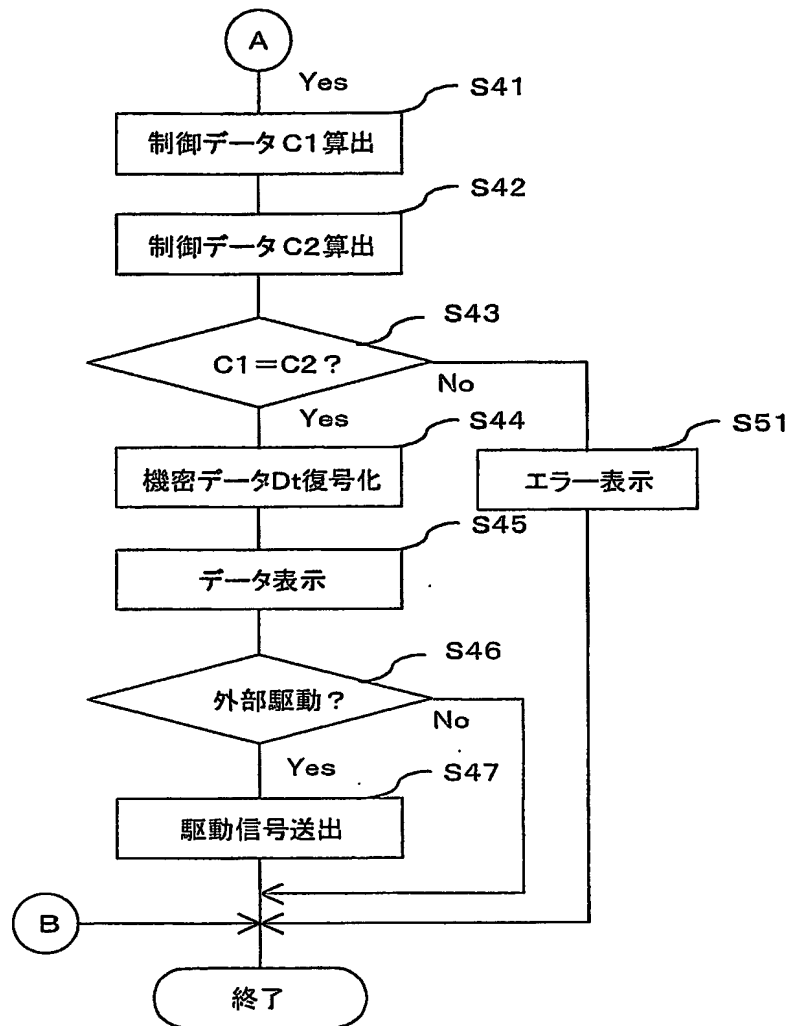
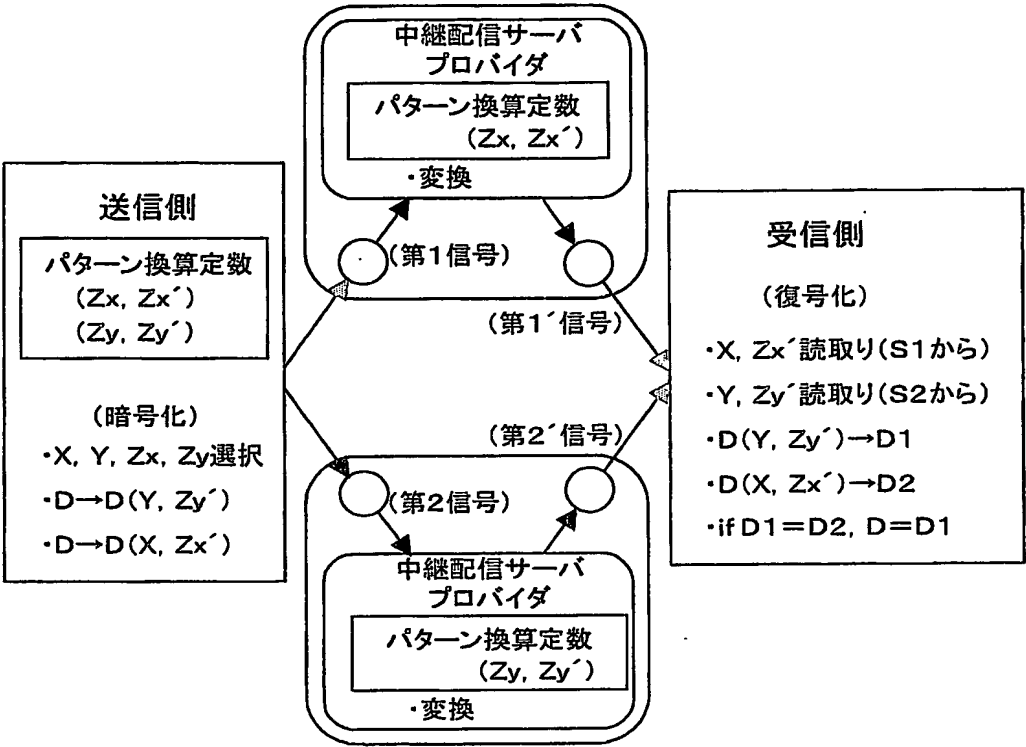


図 17



17/19

図 18

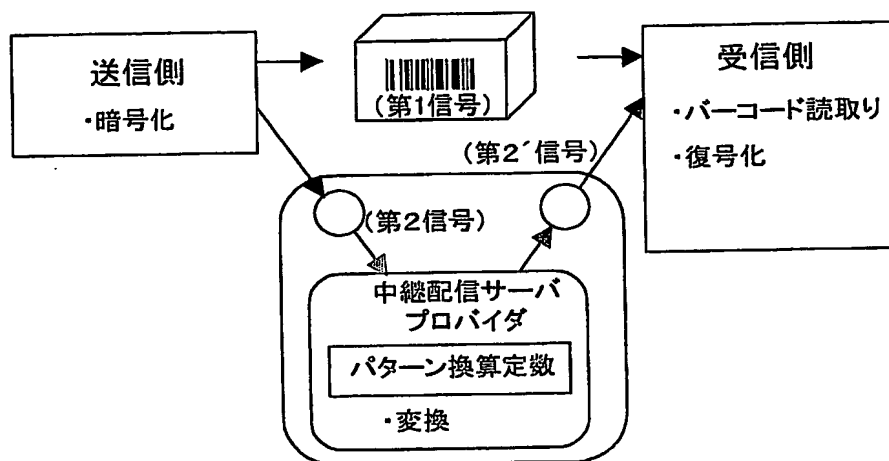


図 19

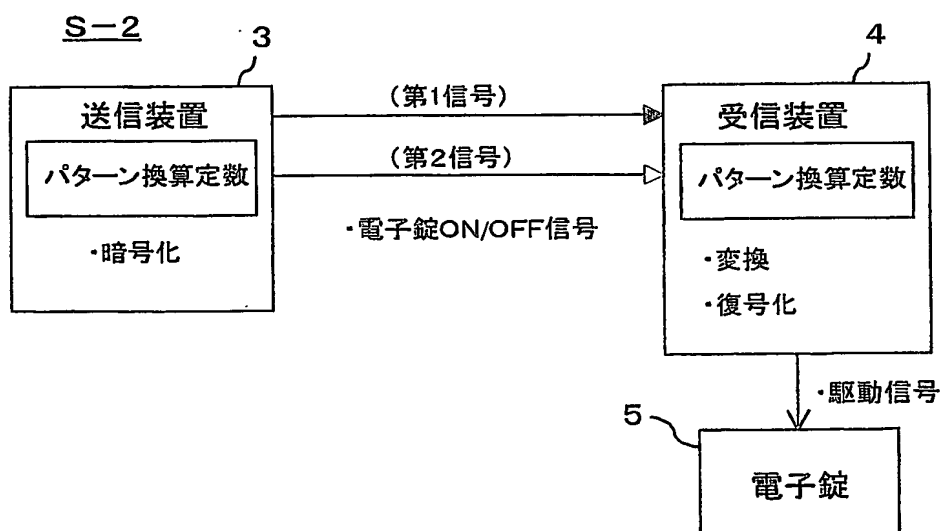
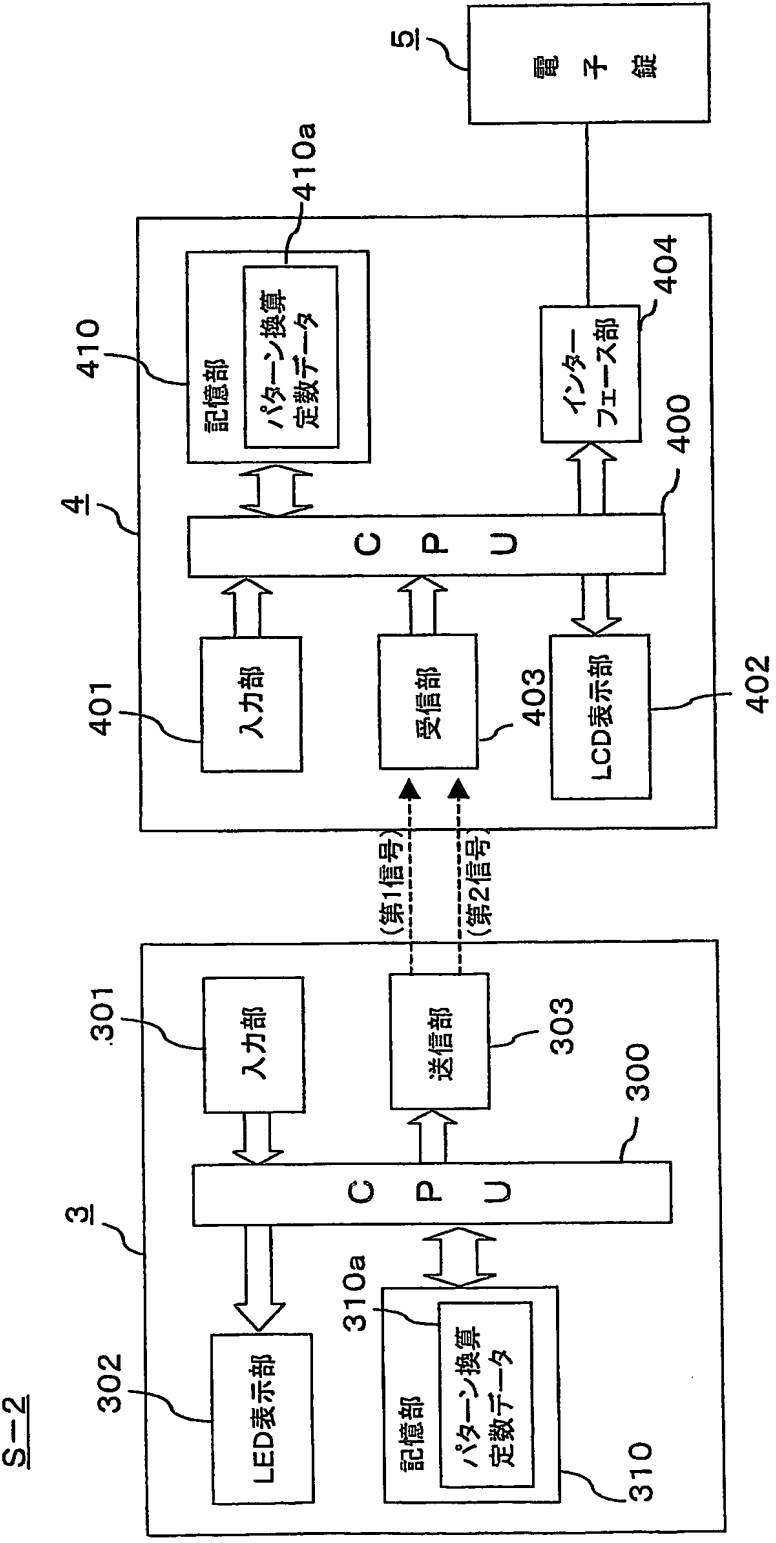


図 20



19/19

図 21

第1信号(暗号化信号) A(個人認証番号):1234 5678 B(ON/OFF信号):1又は0

| 名 称 | 通信 番号 | 換算 定数 | 個人ID 代替値 | ON/OFF 信号 | |
|--------------------|----------|----------|-------------|--------------|---|
| パケット 番号 (PK No) | 0 | 1 | 2 | 3 | 4 |
| Signal | T No | X | | Ax | B |
| データ入力例 | 001 | 1122 | | 1235 2421 | 1 |

$Ax = (A+Y+Zy')$ ON信号

図 22

第2信号(暗号化信号) A(個人認証番号):1234 5678 B(ON/OFF信号):1又は0

| 名 称 | 通信 番号 | 換算 定数 | パターン 換算定数 | 個人ID 代替値 | |
|--------------------|----------|----------|--------------|-------------|---|
| パケット 番号 (PK No) | 0 | 1 | 2 | 3 | 4 |
| Signal | T No | Y | Zy | Ay | |
| データ入力例 | 001 | 3344 | g | 1235 0199 | |

Ay =
g=3399

(A+X+Zy')